МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение
высшего профессионального образования

«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ
ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»

Э. А. Мухутдинов, С. Ю. Ситников, Е. А. Комиссарова

МИРОВЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ И СЕТИ

Учебное пособие

Казань 2007

УДК 681.3
С 41

Мухутдинов Э. А., Ситников С. Ю., Комиссарова Е. А.

Мировые информационные ресурсы и сети: Учебное пособие. / Э. А. Мухутдинов, С. Ю. Ситников, Е. А. Комиссарова. – Казань: Изд-во Казан. гос. энерг. ун-та, 2007. – 238 с.

В учебном пособии даны сведения об организации вычислительных сетей, об их архитектуре, основных моделях, протоколах и стеках протоколов. Подробно раскрыты основные характеристики сетей – от локальных до глобальных. Приведены примеры глобальных сетей, показано их влияние на формирование главной глобальной сети современной цивилизации – интернета. Даны основные хронологические этапы становления интернета начиная от зарождения идеи децентрализованной сети до сегодняшнего дня. Рассмотрены различные сервисы, доступные в интернете, а также приведены описания некоторых технологий, составляющих основу глобальной сети. Для лучшего понимания проблем, стоящих перед организацией вычислительных сетей и взаимодействия компьютеров и пользователей в них даны основы информационной безопасности в применении к компьютерным сетям.

В пособии приведено большое количество терминов и понятий, специфичных для вычислительных сетей, а также раскрыты их происхождение и смысл. Последнее важно для понимания сетевой специфики и призвано способствовать более глубокому усвоению предмета.

Учебное пособие предназначено для студентов специальностей 032001.65 «Документоведение и документационное обеспечение управления» и 200106.65 «Информационно-измерительная техника и технологии», а также окажется весьма полезным для всех студентов, сотрудников и преподавателей при более близком знакомстве с сетевыми технологиями.

Подготовлено на кафедре информатики и информационных управляющих систем.

Печатается по решению редакционно-издательского совета Казанского государственного энергетического университета.

Рецензенты:
первый {???}
второй {???}

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В наше время обособленный компьютер постепенно становится анахронизмом. Если с него нельзя выйти в интернет, подключиться к локальной сети или хотя бы к другому компьютеру, то функциональность его как универсального инструмента сильно уменьшается. Следует отметить, что объединять компьютеры в сеть начали еще в середине прошлого века, как только стало ясно, что таким образом можно достичь увеличения суммарной производительности если не самих компьютеров, то людей, работающих за ними. Тем не менее, только в последнее десятилетие, с активным наступлением эры информационных технологий и повальным проникновением в повседневную жизнь глобальных сетей, и в первую очередь – интернета[1], становится ясно, что всеобщее «осетенение» неизбежно. Кроме того, все больше появляется обычных бытовых устройств, снабженных средствами управления через компьютерные сети, так, в некоторых странах уже нередко встречаются холодильники с блоком управления через интернет и вынесенным на наружную стенку дверцы монитором для удобного путешествия по сети. Воспринимаемые ранее как забавные курьезы, подобные нововведения постепенно внедряются в обыденную жизнь. Этот процесс происходит неторопливо, но уверенно, и, возможно, уже через десять лет мы будем спокойно отдавать команды домашней технике по сети, находясь еще на работе, – точно так же, как сегодня спокойно разговариваем по мобильному телефону, не задумываясь, что всего лет десять-пятнадцать тому назад они были не то что роскошью, а только-только появились.

В этих условиях специалисту необходимо знать основы существования глобальных сетей. Наполнение их информационными ресурсами существенно зависит от технических аспектов функционирования и, к сожалению, на данный момент не существует идеальных способов создания, публикации и

[1] Согласно действующим правилам русского языка и в соответствии со словарями русского языка, слово «Интернет» – имя собственное, соответственно, пишется с прописной буквы, мужского рода, склоняется. Однако русский язык постоянно и динамично развивается. Учитывая, что интернет стал единой, всемирной, общераспространенной информационной сетью, таким же общепринятым средством передачи информации, как, например, телефон, то написание его с прописной буквы можно считать весьма спорным. В настоящее время еще не принято окончательного решения по этому вопросу, выдвигаются аргументы как «за», так и «против». В данном учебном пособии мы будем придерживаться написания слова со строчной буквы, имея при этом в виду, что речь может идти как о среде передачи данных, так и о конгломерате вычислительных сетей.

поиска информации в сетях. По сути, все применяемые методы являются компромиссом между способами, эффективными с точки зрения скорости, с точки зрения надежности, с точки зрения безопасности, с точки зрения экономности и так далее. Выигрывая в надежности, неизбежно получим проигрыш в скорости, и наоборот. Универсальных же решений нет и, скорее всего, не будет никогда, поскольку сплав множества технологий, который являют собой информационные сети, не только тянет за собой массу прежних разработок, требующих обратной совместимости, но и обладает колоссальной инерцией. Понимание того, что нужно сделать для улучшения функционирования сети, зачастую приходит уже после того, как реализована основная часть запланированных работ, и начали всплывать подводные камни, до того неочевидные.

Следует уверенно помнить, что мировые информационные сети в наше время стали гигантской библиотекой человеческих знаний и опыта. С другой стороны, их не зря называют «громадной помойкой», поскольку ценные крупицы упомянутого знания и опыта в некоторой предметной области, изложенные в электронной форме и доверенные магнитному или оптическому носителю, еще необходимо отыскать среди бесчисленного множества информации, относящейся к другой отрасли знаний или вовсе обладающей нулевой ценностью. Специалист, разбирающийся в базовых принципах функционирования сетей и имеющий представление о том, как, где и зачем содержится информация в информационных сетях, получает преимущество перед другим специалистом, такими знаниями не обладающим. А в условиях профессиональной конкуренции это немаловажный фактор.

В данном учебном пособии изложены основы построения вычислительных сетей и приведены подробные примеры глобальных сетей различного типа. Предложены также некоторые сведения о языках разметки, являющихся основным средством публикации текстовой информации в современных сетях. Напоследок затронуты некоторые правовые аспекты применения информации и вопросы безопасности ее использования. Помимо этого, в пособии приведено множество пояснений для терминов, которые в информационной среде считаются обыденными, но начинающему специалисту могут быть еще не знакомы.

1. МИРОВЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ И СЕТИ

1.1. Эволюция вычислительных систем

Вычислительные сети являются логическим результатом эволюции компьютерной технологии. Первые компьютеры появились в 40-50-х годах и предназначались для решения баллистических задач. В таких компьютерах не была предусмотрена интерактивная работа с пользователем, а применялся режим *пакетной обработки*[2]. Системы пакетной обработки обычно строились на базе мэйнфреймов – мощных компьютеров универсального назначения. Пользователи подготавливали перфокарты, содержащие данные и команды программ, и передавали их в вычислительный центр. Специально обученные операторы вводили эти карты в компьютер, а распечатанные результаты пользователи получали на следующий день.

В начале 60-х годов начали развиваться интерактивные *многотерминальные* системы разделения времени. В таких системах каждый пользователь получал в свое распоряжение терминал, с помощью которого мог вести диалог с компьютером. Время реакции вычислительной системы было достаточно мало для того, чтобы пользователю была не слишком заметна параллельная работа с компьютером других пользователей. Терминалы уже не были сосредоточены в вычислительном центре, а могли быть распределены по всему предприятию. И хотя вычислительная мощность оставалась централизованной, функции ввода-вывода данных стали распределенными. Такие многотерминальные централизованные системы стали первым шагом на пути создания локальных вычислительных сетей.

Однако реальная потребность в локальных сетях в это время еще не назрела. Первоначально появилась потребность в соединении компьютеров, находящихся на большом расстоянии друг от друга. Решалась простая задача – доступ к компьютеру с терминала, удаленного на сотни километров. Такие

[2] Пакетная обработка – один из самых простых методов автоматизации компьютерного труда. Суть ее заключается в том, что компьютеру единовременно выдается «заказ» на то, чтобы одинаковым заранее оговоренным способом обработать несколько объектов одного типа. Как правило, пакетная обработка применяется в том случае, когда необходимо выполнить много однообразных действий. Однако встречаются и более сложные задачи, требующие применения языков программирования. Классический пример – пакетные задания, запускаемые автоматически раз в день, неделю и месяц в ОС Unix – такие задания выполняют массу работы по обслуживанию системы и выявлению возможных проблем.

терминалы соединялись с компьютерами через телефонные сети с помощью модемов, что позволяло получать удаленный доступ к ресурсам компьютеров класса супер-ЭВМ. Затем появились системы, в которых наряду с удаленными соединениями типа терминал–компьютер были реализованы и удаленные связи типа компьютер–компьютер.

В начале 70-х годов были разработаны большие интегральные схемы, на основе которых стали создаваться мини-ЭВМ, экономически более выгодные, нежели супер-ЭВМ. Мини-компьютеры выполняли задачи управления технологическим оборудованием, складом и другие задачи уровня подразделения предприятия. Возникла потребность объединения мини-компьютеров предприятия вместе и разработки программного обеспечения, необходимого для их взаимодействия.

В результате появились *локальные вычислительные сети*. На первых порах для соединения компьютеров друг с другом использовались разнообразные нестандартные устройства со своими способами представления данных на линиях связи. Эти устройства могли соединять только те типы компьютеров, для которых были разработаны. Разумеется, такая ситуация мешала повсеместному внедрению локальных вычислительных сетей и, кроме того, ограничивала выбор для каждой организации только одним производителем.

В середине 80-х годов были созданы стандартные технологии объединения компьютеров в сеть – Ethernet, Arcnet, Token Ring. Персональные компьютеры оказались идеальными элементами для построения сетей: с одной стороны, они стали достаточно мощными для работы сетевого программного обеспечения, а с другой – явно нуждались в объединении вычислительной мощности для решения сложных задач и разделения дорогих периферийных устройств и дисковых массивов.

На сегодняшний день для создания сети достаточно приобрести сетевые адаптеры соответствующего стандарта и кабель, присоединить адаптеры к кабелю стандартными разъемами и установить на компьютер одну из сетевых операционных систем. После этого сеть начинает работать, и присоединение каждого нового компьютера не вызывает особых проблем. По этим и некоторым другим причинам вычислительные сети быстро развиваются. Следует отметить, что различия между локальными и глобальными сетями постоянно уменьшаются из-за появления высокоскоростных территориальных каналов связи. В глобальных сетях появляются службы (сервисы) досту-

па к ресурсам, близкие по потребительским характеристикам к аналогичным службам локальных сетей.

Появилась еще одна важная тенденция, затрагивающая в равной степени и локальные, и глобальные сети. В них стала обрабатываться несвойственная ранее вычислительным сетям информация – *мультимедийная*, включающая в себя звук, видеоизображения, рисунки. Это потребовало внесения существенных изменений в работу протоколов, сетевых операционных систем и коммуникационного оборудования.

1.2. Распределенные вычислительные системы

Если вычислительная система содержит несколько центров обработки информации, то она называется *распределенной вычислительной системой*. К таким системам относятся компьютерные сети, многомашинные вычислительные комплексы и даже мультипроцессорные компьютеры.

Часто возникает путаница между *распределенными системами* и *сетями ЭВМ*. Работая с распределенной системой, пользователь может не иметь ни малейшего представления, на каких процессорах и с использованием каких ресурсов будет исполняться его программа.

В сети, поскольку все машины там автономны, пользователь должен делать все явно. Основное различие между этими системами лежит в организации их программного обеспечения. И там, и там происходит передача информации. Вопрос в том, кто ее инициирует. В сети – пользователь, в распределенной системе – система.

Основным признаком распределенной вычислительной системы является наличие нескольких центров обработки данных, что дает возможность распараллелить вычисления. Поэтому к распределенным системам относят также мультипроцессорные компьютеры и многомашинные вычислительные комплексы.

В *мультипроцессорных компьютерах*[3] имеется несколько процессоров,

[3] Следует отметить, что в настоящее время развитие процессорных систем по пути наращивания тактовой частоты достигло обозримого физического предела. Дальнейшее увеличение частоты сопряжено с необходимостью отвода значительного количества тепла от нагревающегося микропроцессора. Одним из выходов является дальнейшее совершенствование производственных процессов и переход на все более малые технологические размеры. Однако этот путь достаточно нетороплив, поскольку такой переход требует существенных затрат времени и средств. Другой подход, в настоящее время представляю-

каждый из которых может относительно независимо от остальных выполнять свою программу. В таком компьютере существует общая для всех процессоров операционная система, которая оперативно распределяет вычислительную нагрузку между ними. Взаимодействие между отдельными процессорами организуется наиболее простым способом – через общую оперативную память.

Основное достоинство мультипроцессорного компьютера – его высокая производительность, достигаемая за счет параллельной работы нескольких процессоров. Так как при наличии общей памяти взаимодействие процессоров происходит очень быстро, могут эффективно выполняться специально разработанные приложения с высокой степенью связи по данным. Еще одним важным свойством мультипроцессорных систем является отказоустойчивость, то есть способность к продолжению работы при физических отказах некоторых элементов, например процессоров или блоков памяти. При этом производительность, естественно, снижается, но не до нуля, как в обычных системах, в которых отсутствует избыточность.

Многомашинная система (*кластер*) – это вычислительный комплекс, включающий в себя несколько компьютеров, каждый из которых работает под управлением собственной операционной системы, а также программные и аппаратные средства связи компьютеров, обеспечивающие работу всех компьютеров комплекса как единого целого. Многомашинные комплексы характеризуются высокими отказоустойчивостью и производительностью.

Вычислительная сеть – это совокупность компьютеров, соединенных линиями связи. В вычислительных сетях программные и аппаратные связи являются еще более слабыми, а автономность обрабатывающих блоков проявляется в наибольшей степени. Основными элементами сети являются стандартные компьютеры, не имеющие ни общих блоков памяти, ни общих периферийных устройств.

щийся более перспективным, – внедрение в широкое использование многопроцессорных систем. Переход на них начался с появления процессоров Intel Pentium IV с технологией HyperThreading, которая позволяла один микропроцессор представить для системы как два. В дальнейшем появление двух- (Intel Pentium D, Intel Core 2 Duo, AMD Athlon 64 X2), четырехъядерных (Intel Xeon 5300, Intel Quad Core, Intel Yorkfield, AMD Quad K8L, AMD Altair FX) и более (в начале 2007 года корпорация Intel представила экспериментальный образец 80-ядерного процессора производительностью 1 терафлоп – триллион операций с вещественными числами в секунду) процессоров вкупе с агрессивной маркетинговой политикой привели к востребованности таких систем на широком потребительском рынке.

Использование вычислительных сетей дает предприятию следующие возможности:

- разделение (то есть совместное использование) дорогостоящих ресурсов (например, дисковой памяти);
- совершенствование коммуникаций;
- улучшение доступа к информации;
- свобода в территориальном размещении компьютеров.

Основная цель любой сети – обеспечить пользователям возможность совместного использования ресурсов всех компьютеров. На тех компьютерах, ресурсы которых должны быть доступны всем пользователям сети, необходимо добавить программные модули, которые постоянно будут находиться в режиме ожидания запросов, поступающих по сети от других компьютеров. Обычно такие модули называются *программными серверами*, так как их главная задача – обслуживать запросы на доступ к ресурсам своего компьютера. На компьютерах, пользователи которых хотят получить доступ к ресурсам других компьютеров, также нужно добавить к операционной системе программные модули, которые вырабатывают запросы на доступ к удаленным ресурсам и передают их по сети на нужный компьютер. Такие модули обычно называют программными *клиентами*[4].

Пара модулей «клиент–сервер» обеспечивает совместный доступ пользователей к определенному типу ресурсов, например, к файлам или принтерам. В этом случае говорят, что пользователь имеет дело с файловой *службой* (*service*). Обычно сетевая операционная система поддерживает несколько видов сетевых служб для своих пользователей – файловую службу, службу печати, службу электронной почты, службу удаленного доступа и т. п.

Сетевые службы всегда представляют собой распределенные программы. *Распределенная программа* – это программа, состоящая из нескольких взаимодействующих частей, причем каждая часть, как правило, выполняется на отдельном компьютере сети.

Кроме *системных* распределенных программ, в сети могут выполняться и распределенные *пользовательские программы – сетевые приложения*.

[4] Термины «клиент» и «сервер» используются не только для обозначения программных модулей, но и компьютеров, подключенных к сети. Если компьютер предоставляет свои ресурсы другим компьютерам сети, то он называется сервером, а если потребляет – клиентом. Иногда один и тот же компьютер может одновременно играть роли и сервера, и клиента.

Распределенное приложение также состоит из нескольких частей, каждая из которых выполняет какую-то определенную законченную работу по решению прикладной задачи. Например, одна часть приложения (клиентская), может поддерживать пользовательский интерфейс, вторая – заносить полученные результаты в базу данных (серверная, работающая на компьютере с установленной стандартной СУБД[5]).

1.3. Структура функционирования сети. Эталонная модель ISO OSI

Современные сети построены по многоуровневому принципу. Чтобы организовать связь двух компьютеров, требуется сначала создать свод правил их взаимодействия, определить язык общения, т.е. установить, что означают посылаемые ими сигналы и т.д. Формализованные правила и соглашения, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах, называются *протоколом*.

В начале 80-х годов ряд международных организаций по стандартизации – ISO[6], ITU-T и некоторые другие – разработали модель взаимодействия двух систем, названную эталонной моделью ISO OSI[7], определяющую различные уровни, дающую им стандартные имена и указывающую, какие функции должен выполнять каждый уровень. В этой модели (рис. 1) средства взаимодействия делятся на семь уровней: прикладной, представительный, сеансовый, транспортный, сетевой, канальный и физический. Каждый уровень

---

[5] СУБД – система управления базами данных.

[6] ISO – International organization for standardization, Международная организация по стандартизации. Создана в 1947 г. В настоящее время в нее входят свыше 100 стран. Цель ISO – развитие принципов стандартизации и проектирование на их основе стандартов, способствующих интеграционным процессам в разных областях и направлениях человеческой деятельности.

Инициатива создания новых стандартов исходит от организаций, использующих стандарты (как правило, это производитель продукции или услуг, нуждающихся в их интеграции с другой продукцией или услугами). Эти организации формируют базовые требования к стандарту и передают их своим национальным представителям в ISO. В ISO решается вопрос о целесообразности разработки новых стандартов. В случае положительного решения определяется технический комитет, которому предстоит разработать проект стандарта. Далее проект рассылается в адреса комитетов членов ISO для изучения и оценки. После положительных итогов голосования он принимается как стандарт ISO. Разработка стандарта занимает около 7 лет.

[7] OSI – Open system interconnection, взаимодействие открытых систем.

имеет дело с одним определенным аспектом взаимодействия сетевых устройств, каждому из них соответствует свой стек протоколов.

Стек протоколов – это иерархически организованный набор коммуникационных протоколов, достаточный для организации взаимодействия узлов в сети.

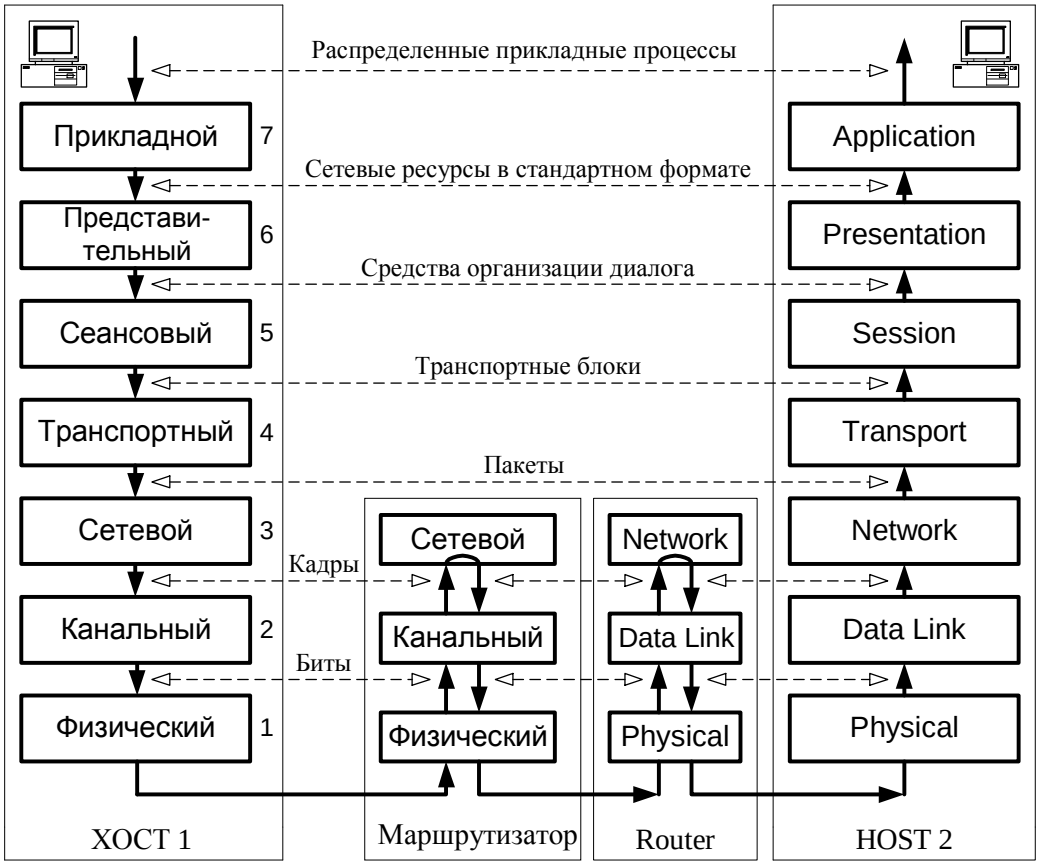


Рис. 1. Эталонная модель ISO OSI.

Принципы выделения этих уровней таковы:

- каждый уровень отражает надлежащий уровень абстракции;
- каждый уровень имеет строго определенную функцию;
- эта функция выбиралась, прежде всего, так, чтобы можно было определить международный стандарт;
- границы выбирались так, чтобы минимизировать поток информации через интерфейсы;
- число уровней должно быть достаточно большим, чтобы не объединять разные функции на одном уровне, и оно должно быть достаточно малым, чтобы архитектура не была громоздкой.

Рассмотрим каждый уровень модели. Отметим что это именно модель, а не архитектура сети. Она не определяет протоколы и сервис каждого уров-

ня, а лишь говорит, что он должен делать. ISO выпустила также стандарты для каждого уровня, но они не являются частью модели.

Уровень среды передачи данных

Этот уровень связан с физической средой – передатчиком сигнала и на самом деле не включается в схему. Он представляет посредники, соединяющие конечные устройства: кабели, радиолинии и т.д. Кабелей существует великое множество различных видов и типов: экранированные и неэкранированные витые пары, коаксиальные, на основе оптических волокон и т. д. Так как этот уровень не включен в схему, он ничего не описывает, а только указывает на среду.

Физический уровень

Физический уровень (*Physical layer*) имеет дело с передачей битов по физическим каналам связи, таким, как коаксиальный кабель, витая пара, оптоволоконный кабель или радиоканал. К этому уровню имеют отношение характеристики физических сред передачи данных, такие как полоса пропускания, помехозащищенность, волновое сопротивление и другие. На этом же уровне определяются характеристики электрических сигналов, передающих дискретную информацию, например, крутизна фронтов импульсов, уровни напряжения или тока передаваемого сигнала, тип кодирования, скорость передачи сигналов. Кроме этого, 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.

Канальный уровень

Одной из задач канального уровня (*Data link layer*) является *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, для его выделения

(определения границ кадра), а также вычисляет контрольную сумму, обрабатывая все байты кадра определенным способом и добавляя контрольную сумму к кадру.

Помехи на линии могут разрушить фрейм. В этом случае он должен быть передан повторно. Он будет повторен также и в том случае если фрейм-уведомление будет потерян. Когда кадр приходит по сети, 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. Канальный уровень может не только обнаруживать ошибки, но и исправлять их за счет повторной передачи поврежденных кадров.

Другой проблемой, возникающей на уровне канала данных (равно как и на других вышележащих уровнях) является *управление потоком (flow control)* передачи. Например, если устройство коммутации обладает функцией управления *трафиком*[8], то это препятствует блокированию его портов и обеспечивает уменьшение потоков данных на входных портах, если выходные перегружены.

В сетях с *вещательным* способом передачи возникает проблема управления доступом к общему каналу. В соответствии со стандартом IEEE 802 канальный уровень делится на два подуровня:

- нижний подуровень доступа к среде (*Media access control, MAC*). MAC-подуровень осуществляет прямой доступ к среде передачи информации (каналу связи). Он напрямую связан с аппаратурой сети;
- верхний подуровень (*Logical link control, LLC*) осуществляет управление логической связью, то есть устанавливает виртуальный канал связи (часть его функций выполняется программным драйвером сетевого адаптера).

Уровень MAC появился из-за существования в локальных сетях разделяемой среды передачи данных. Именно этот уровень обеспечивает корректное совместное использование общей среды, предоставляя ее в соответствии с определенным алгоритмом в распоряжение той или иной станции сети. После того как доступ к среде получен, ею может пользоваться более высокий уровень – уровень LLC, организующий передачу логических единиц данных, кадров информации, с различным уровнем качества транспортных услуг. В современных локальных сетях получили распространение несколько протоколов уровня

[8] Трафик – информация, передаваемая по линиям связи.

MAC, реализующих различные алгоритмы доступа к разделяемой среде. Эти протоколы полностью определяют специфику таких технологий, как Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, l00VG-AnyLAN.

Уровень LLC отвечает за передачу кадров между узлами с различной степенью надежности, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем. Именно через уровень LLC сетевой протокол запрашивает у канального уровня нужную ему транспортную операцию с нужным качеством. Здесь существует несколько режимов работы, отличающихся наличием или отсутствием на этом уровне процедур восстановления кадров в случае их потери или искажения, то есть отличающихся качеством транспортных услуг этого уровня.

Протоколы уровней MAC и LLC взаимно независимы – каждый протокол уровня MAC может применяться с любым протоколом уровня LLC, и наоборот.

В протоколах канального уровня, используемых в локальных сетях (например – Ethernet), заложена 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 той *топологией*[9], для которой он был разработан. К таким типовым топологиям, поддерживаемым протоколами канального уровня локальных сетей, относятся общая шина, кольцо и звезда, а также структуры, полученные из них с помощью мостов и коммутаторов.

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

В глобальных сетях, которые редко обладают регулярной топологией, канальный уровень часто обеспечивает обмен сообщениями только между двумя соседними компьютерами, соединенными индивидуальной линией связи. Примером протокола «точка–точка» может служить протокол PPP.

Для обеспечения качественной транспортировки сообщений в сетях любых топологий и технологий функций канального уровня оказывается недостаточно, поэтому в модели OSI решение этой задачи возлагается на два следующих уровня – сетевой и транспортный.

[9] Топология – способ организации физических связей в сети.

Сетевой уровень

Сетевой уровень (*Network layer*) служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать совершенно различные принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей.

На сетевом уровне сам термин *сеть* наделяется специфическим значением. В данном случае под сетью понимают 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.

Внутри сети доставка данных обеспечивается соответствующим канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора маршрута передачи сообщения даже в том случае, когда структура связей между составляющими сетями имеет характер, отличный от принятого в протоколах канального уровня. 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 между сетями*, или *хопов* (от *hop* – прыжок), каждый раз выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, через которые проходит пакет.

Сетевой уровень отвечает за функционирование подсети. Основной проблемой здесь является – как маршрутизировать пакеты от отправителя к получателю. Маршруты могут быть определены заранее и прописаны в статической *таблице маршрутизации*, которая не изменяется. Они могут определяться в момент установления соединения. Наконец, они могут строиться динамически в зависимости от загрузки сети.

Если в подсети циркулирует слишком много пакетов, то они могут использовать одни и те же маршруты, что будет приводить к заторам. Эта проблема так же решается на сетевом уровне.

Проблема выбора наилучшего пути называется *маршрутизацией*, и ее решение является одной из главных задач сетевого уровня. Эта проблема ос-

ложняется тем, что самый короткий путь не всегда самый лучший. Часто критерием при выборе маршрута является время передачи данных по этому маршруту; оно зависит от пропускной способности каналов связи и интенсивности трафика, которая может изменяться с течением времени.

Сообщения сетевого уровня принято называть *пакетами (packets)*.

На сетевом уровне определяются два вида протоколов. Первый вид – *сетевые протоколы (routed protocols)* – реализуют продвижение пакетов через сеть. Именно эти протоколы обычно имеют в виду, когда говорят о протоколах сетевого уровня. Однако часто к сетевому уровню относят и другой вид протоколов, называемых протоколами обмена маршрутной информацией или просто *протоколами маршрутизации (routing protocols)*. 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.

На сетевом уровне работают протоколы еще одного типа, которые отвечают за отображение адреса узла, используемого на сетевом уровне, в локальный адрес сети. Такие протоколы часто называют *протоколами разрешения адресов (Address resolution protocol, ARP)*. Иногда их относят не к сетевому уровню, а к канальному, хотя тонкости классификации не изменяют их сути.

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

В сетях с вещательной передачей проблемы маршрутизации просты, и этот уровень часто отсутствует.

Транспортный уровень

Основная функция транспортного уровня (*Transport layer*) это: принять данные с уровня сессии, разделить, если надо, на более мелкие единицы, передать на сетевой уровень и позаботиться, чтобы все они дошли в целостности до адресата.

В нормальных условиях транспортный уровень должен создать специальное сетевое соединение для каждого транспортного соединения по запросу уровня сессии (сеанса). Если транспортное соединение требует высокой

пропускной способности, то транспортный уровень может создать несколько сетевых соединений, между которыми транспортный уровень буден распределять передаваемые данные. И наоборот, если требуется обеспечить недорогое транспортное соединение, то транспортный уровень может использовать одно и то же сетевое соединение для нескольких транспортных соединений. В любом случае, такое мультиплексирование должно быть незаметным на уровне сессии.

Транспортный уровень также отвечает за установление и разрыв транспортного соединения в сети. Это предполагает наличие механизма именования, т.е. процесс на одной машине должен уметь указать с кем в сети ему надо обменяться информацией. Транспортный уровень также должен предотвращать перегрузку получателя в случае очень «быстро говорящего» отправителя. Этот механизм – управление потоком – есть и на других уровнях. Однако механизм управления потоком между *хостами*[10] отличен от управление потоком между маршрутизаторами.

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. Транспортный уровень обеспечивает 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[11]: 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.

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 про-

---

[10] Host – хозяин, принимающая сторона (*англ.*). В терминологии вычислительных сетей хостом называют любой компьютер или устройство, подключенное к сети и имеющее собственный адрес, уникальный в пределах данной сети.

[11] QoS – Quality of service, качество обслуживания.

токолов можно привести протоколы TCP и UDP стека TCP/IP и протокол SPX стека Novell.

Протоколы нижних четырех уровней обобщенно называют сетевым транспортом или транспортной подсистемой, так как они полностью решают задачу транспортировки сообщений с заданным уровнем качества в составных сетях с произвольной топологией и различными технологиями. Остальные три верхних уровня решают задачи предоставления прикладных сервисов на основании имеющейся транспортной подсистемы.

Сеансовый уровень

Сеансовый уровень (*Session layer*) позволяет пользователям на разных машинах (пользователем может быть программа) устанавливать *сессии* (*сеансы*). Сессия позволяет передавать данные, как это может делать транспортный уровень, но также этот уровень имеет более сложный сервис, полезный в некоторых приложениях. Например, вход в удаленную систему, передача файла между двумя приложениями.

Один из видов услуг на сеансовом уровне – управление диалогом. Потоки данных могут быть разрешены в обоих направлениях одновременно, либо поочередно в одном направлении. Сервис на уровне сессии будет управлять направлением передачи.

Другой услугой уровня сессии является *синхронизация*. Она позволяет вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все с начала.

Представительный уровень

Представительный (или представительский) уровень (*Presentation layer*) имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например кодов ASCII и UNICODE. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обес-

печивается сразу для всех прикладных служб. Примером такого протокола является протокол SSL[12], который обеспечивает обмен криптографически закрытыми сообщениями для протоколов прикладного уровня стека TCP/IP.

Прикладной уровень

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

Существует очень большое разнообразие служб прикладного уровня. Наиболее распространенные реализации файловых служб: SMB в Microsoft Windows NT; NFS и FTP, входящие в стек TCP/IP.

Сетезависимые и сетенезависимые уровни

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*, то есть протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием. Например, переход на оборудование ATM означает полную смену протоколов физического и канального уровней во всех узлах сети.

Три верхних уровня – прикладной, представительный и сеансовый – ориентированы на приложения и мало зависят от технических особенностей построения сети, т.е. являются *сетенезависимыми*

На протоколы этих уровней не влияют какие бы то ни было 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. Это позволяет разраба-

[12] SSL – Secure sockets layer, протокол защищенных портов. Протокол, гарантирующий безопасную передачу данных по сети, комбинирует криптографическую систему с открытым ключом и блочное шифрование данных.

тывать приложения, не зависящие от технических средств транспортировки сообщений. Компьютер с установленной на нем *сетевой операционной системой* (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), либо на физическом, канальном и сетевом, иногда захватывая и транспортный уровень (маршрутизатор). На рис. 2 показано соответствие функций различных коммуникационных устройств уровням модели OSI.

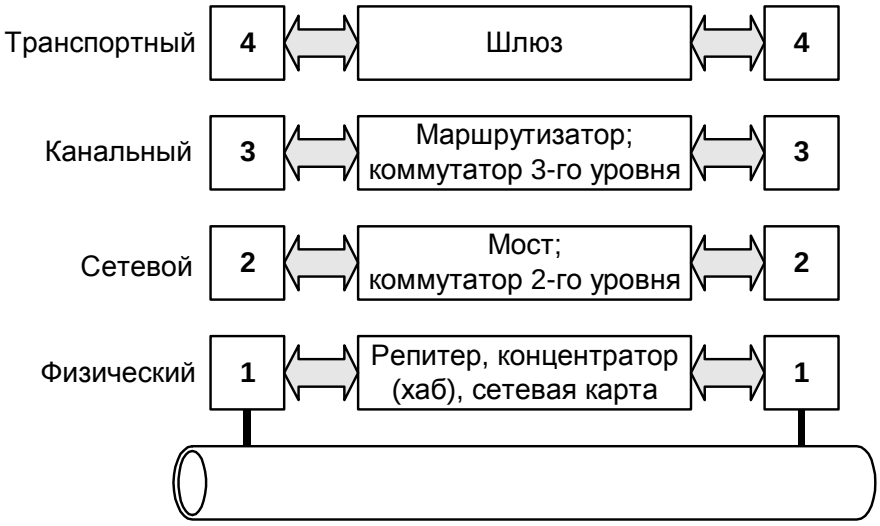


Рис. 2. Соответствие функций различных устройств сети уровням модели OSI

Многоуровневая структура ISO OSI спроектирована с целью упорядочить множество протоколов и отношений. Она позволяет составлять сетевые системы из модулей программного обеспечения, выпущенных самыми разными производителями. Заложенное в названии модели понятие «взаимодействие открытых систем» не случайно. *Открытая система* – это любая система (компьютер, вычислительная сеть, операционная система, программный пакет), которая построена в соответствии с открытыми (общедоступными) спецификациями[13], соответствующими стандартам и принятыми в результате публичного обсуждения всеми заинтересованными сторонами[14]. Использование при разработке систем открытых спецификаций позволяет третьим сто-

[13] Спецификация – формализованное описание аппаратных или программных компонентов, способов их функционирования, взаимодействия с другими компонентами.

[14] В данном случае это ISO.

ронам разрабатывать для этих систем различные аппаратные или программные средства расширения и модификации, а также создавать программно-аппаратные комплексы из продуктов разных производителей.

Ярким примером открытой системы является интернет. Эта сеть развивалась в соответствии с требованиями, предъявляемыми к открытым системам. В разработке ее стандартов принимали участие специалисты из различных университетов, научных организаций и фирм-производителей вычислительной аппаратуры и программного обеспечения, работающих в разных странах. Название стандартов, определяющих работу интернета – *Request for comments* (*RFC*), что переводится как «запрос на комментарии», – показывает гласный и открытый характер принимаемых стандартов. В результате интернет сумел объединить в себе самое разнообразное оборудование и программное обеспечение огромного числа сетей, распределенных по всему миру.

В то же время, модель OSI касается только одного аспекта открытости, а именно открытости средств взаимодействия устройств, связанных в вычислительную сеть. Здесь под открытой системой понимается сетевое устройство, готовое взаимодействовать с другими сетевыми устройствами с использованием стандартных правил, определяющих формат, содержание и значение принимаемых и отправляемых сообщений.

Если две сети построены с соблюдением принципов открытости, то это дает следующие преимущества:

- возможность построения сети из аппаратных и программных средств различных производителей, придерживающихся одного и того же стандарта;
- возможность замены отдельных компонентов сети другими, более совершенными, что позволяет сети развиваться с минимальными затратами;
- возможность легкого сопряжения одной сети с другой;
- простота освоения и обслуживания сети.

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, службами, поддерживаемыми на верхних уровнях, и прочими параметрами.

Взаимодействие уровней

Взаимодействие уровней в модели OSI – *субординарное*. Каждый уровень может реально взаимодействовать только с соседними вертикальными

уровнями – верхним и нижним.

Пусть приложение обращается с запросом к прикладному уровню, например к файловой службе. На основании этого запроса программное обеспечение прикладного уровня формирует сообщение стандартного формата. После формирования сообщения прикладной уровень направляет его вниз по стеку представительному уровню. Протокол представительского уровня на основании информации, полученной из заголовка прикладного уровня, выполняет требуемые действия и добавляет к сообщению собственную служебную информацию – заголовок представительного уровня, в котором содержатся указания для протокола представительного уровня машины-адресата. Полученное в результате сообщение передается вниз сеансовому уровню, который в свою очередь добавляет свой заголовок, и т. д. Наконец, сообщение достигает физического уровня, к этому моменту оно обрастает заголовками всех уровней.

Когда сообщение из сети поступает на хост-адресат, оно принимается физическим уровнем и последовательно перемещается вверх с уровня на уровень. Каждый уровень анализирует и обрабатывает заголовок своего уровня, выполняя соответствующие данному уровню функции, а затем удаляет этот заголовок и передает сообщение вышележащему уровню.

Наряду с термином *сообщение (message)* существуют и другие термины, применяемые сетевыми специалистами для обозначения единиц данных в процедурах обмена. В стандартах ISO для обозначения единиц данных, с которыми имеют дело протоколы разных уровней, используется общее название *протокольный блок данных*[15]. Для обозначения блоков данных определенных уровней часто используются специальные названия: бит (*bit*), кадр (*frame*), пакет (*packet*), дейтаграмма (*datagram*), сегмент (*segment*).

Таким образом, модули, реализующие протоколы соседних уровней и находящиеся в одном узле, взаимодействуют друг с другом в соответствии с четко определенными формализованными правилами и с помощью стандартизованных форматов сообщений. Эти правила принято называть *интерфейсом*[16]. Интерфейс определяет набор *сервисов*, предоставляемый данным уровнем соседнему уровню.

---

[15] PDU – Protocol data unit.

[16] Интерфейс – от *interface* (англ.), система связей и взаимодействия устройств компьютера, задает параметры, процедуры и характеристики взаимодействия объектов.

В общем случае, протокол и интерфейс выражают одно и то же понятие, но в сетях за ними закрепили разные области действия: протоколы определяют правила взаимодействия модулей одного уровня в разных узлах (*горизонтальное взаимодействие* по модели OSI), а интерфейсы – модулей соседних уровней в одном узле (*вертикальное взаимодействие*).

Можно сказать, что между каждой парой уровней есть интерфейс, определяющий, какие элементарные операции и какие услуги (сервисы) нижележащий уровень должен обеспечивать для верхнего уровня. Набор уровней и протоколов называется *архитектурой сети*. Спецификация архитектуры сети должна содержать достаточно информации, чтобы разработчик сетевого программного обеспечения мог написать надлежащие программы для каждого уровня, а инженер-электронщик – создать надлежащую аппаратуру.

Средства каждого уровня должны отрабатывать, во-первых, собственный протокол, а во-вторых, интерфейсы с соседними уровнями. Иерархически организованный набор коммуникационных протоколов, достаточный для организации взаимодействия узлов в сети, называется *стеком протоколов*. Обычно имеется в виду конкретный набор протоколов, используемый на конкретной машине.

Коммуникационные протоколы могут быть реализованы программно и аппаратно. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней, как правило, чисто программными средствами.

Модель ISO OSI предписывает очень сильную стандартизацию вертикальных межуровневых взаимодействий. Такая стандартизация гарантирует совместимость продуктов, работающих по стандарту какого-либо уровня, с продуктами, работающими по стандартам соседних уровней, даже в том случае, если они выпущены разными производителями.

1.4. Модель TCP/IP

Рассмотрим другую модель, на которой основано функционирование интернета. С самого начала сеть ARPANET, из которой вырос интернет (подробнее см. гл. 2.9), задумывалась как объединение нескольких разных сетей. Одной из основных целей проекта была разработка унифицированных способов соединения сетей. С появлением спутниковых и радиоканалов связи проблема становилась только актуальнее. Так появилась *модель TCP/IP*. Свое

название она получила по именам двух основных протоколов:

- TCP – Transmission control protocol, или протокол управления передачей;
- IP – Internet protocol, или межсетевой протокол.

Другой целью проекта ARPANET было создание протоколов, не зависящих от характеристик конкретных хост-машин, маршрутизаторов, шлюзов17 и т.п. Кроме того, связь должна поддерживаться, даже если отдельные компоненты сети будут выходить из строя во время соединения. Другими словами, сеть должна работать до тех пор, пока источник информации и получатель информации работоспособны. При этом архитектура сети не должна ограничивать приложения и позволять передачу информации, начиная от простых текстовых файлов до речи и изображения в реальном времени.

Межсетевой уровень

В силу вышеперечисленных требований выбор очевиден: сеть с коммутацией пакетов, использующая сетевой уровень без соединений. Этот уровень называется *межсетевым уровнем*. Он является основой всей архитектуры. Его назначение – обеспечить доставку пакетов, движущихся в сети, независимо друг от друга, даже если получатель принадлежит другой сети. Причем пакеты могут поступать к получателю не в том порядке, в котором они были посланы. Упорядочить их в надлежащем порядке – задача вышележащего уровня.

Межсетевой уровень определяет межсетевой протокол IP и формат пакета. Интересно, что ни протокол, ни формат пакета не являются официальными международными стандартами, в отличие от протоколов модели OSI.

Итак, назначение межсетевого уровня в TCP/IP доставить IP пакет по назначению. Это примерно то, за что отвечает сетевой уровень в модели OSI.

В табл. 1 показано соответствие (достаточно условное) между уровнями этих двух эталонных моделей. Соответствие уровней стека TCP/IP семиуровневой модели OSI показано в табл. 2.

[17] Шлюз – аппаратно-программный комплекс, функционирующий на прикладном уровне модели OSI и передающий данные между несовместимыми прикладными программами или между сетями, использующими различные протоколы.

Таблица 1. Соответствие между уровнями моделей OSI и TCP/IP

	ISO OSI		TCP/IP
7	Прикладной	**I**	Прикладной
6	Представительный		
5	Сеансовый		
4	Транспортный	**II**	Транспортный
3	Сетевой	**III**	Межсетевое взаимодействие
2	Канальный	**IV**	Сетевые интерфейсы
1	Физический		

Таблица 2. Соответствие уровней стека TCP/IP семиуровневой модели OSI

7	WWW[18]	FTP[19]	SMTP[20]	TELNET[21]	SNMP[22]	TFTP[23]	**I**
6							
5	TCP					UDP	**II**
4							
3	IP	RIP[24]	OSPF[25]	ICMP[26]	ARP[27]		**III**
2	Не регламентируется Ethernet, FDDI, X.25, PPP[28]						**IV**
1							
	Уровни модели OSI					Уровни стека TCP/IP	

[18] WWW – World Wide Web, всемирная информационная паутина. В свое время был предложен также забавный русский аналог этого термина – ППП, что значит «повсеместно протянутая паутина».

[19] FTP – File transfer (transport, transition) protocol.

[20] SMTP – Simple mail transfer (transport, transition) protocol.

[21] TELNET – Teletype network, сетевой протокол для удаленного доступа к компьютеру с помощью командного интерпретатора. Аналогичное название имеют утилиты для работы с протоколом. Не использует шифрование, поэтому уязвим для сетевых атак.

[22] SNMP – Simple network management protocol.

[23] TFTP – Trivial file transfer protocol, простейший протокол передачи данных. Упрощенный вариант протокола FTP, поддерживает простую передачу данных между двумя системами без аутентификации.

[24] RIP – Routing information protocol, протокол маршрутной информации. Разработан корпорацией Xerox. Представляет собой протокол динамической распределенной маршрутизации, основанный на алгоритме обмена маршрутными таблицами. Динамический выбор оптимального маршрута обеспечивается периодической рассылкой маршрутизатором широковещательного сообщения, содержащего адреса и расстояния до доступных сетей.

[25] OSPF – Open shortest path first, открытый протокол предпочтения кратчайшего канала. Стандарт протокола маршрутизации, основанный на алгоритме, учитывающем состояние каналов.

[26] ICMP – Internet control message protocol, протокол управляющих сообщений в интернете. Один из четырех протоколов межсетевого уровня семейства TCP/IP, обеспечивает восстановление связи при сбойных ситуациях в передаче пользовательских пакетов.

[27] ARP – Address resolution protocol.

[28] PPP – Point-to-point protocol.

Транспортный уровень

Над межсетевым уровнем расположен транспортный уровень. Как и ISO модели, его задача обеспечить связь «точка–точка» между двумя равнозначными активностями. В рамках модели TCP/IP было разработано два транспортных протокола. Первый – TCP: надежный протокол с соединением. Он получает поток байт, фрагментирует его на отдельные сообщения и передает их на межсетевой уровень. На машине получателе равнозначная активность TCP протокола собирает эти сообщения в поток байтов. TCP протокол также обеспечивает управление потоком.

Второй транспортный протокол – UDP[29]: ненадежный протокол с соединением, используемый для передачи данных в сетях IP и не гарантирующий доставку пакета. Это позволяет ему гораздо быстрее и эффективнее доставлять данные для приложений, которым не требуется большая пропускная способность линий связи, либо требуется малое время доставки данных. В отличие от TCP, UDP используется для широковещательной и многоадресной рассылки.

Уровень приложений

В модели TCP/IP нет уровней сессии и представления. Необходимость в них была неочевидна для ее создателей. На сегодня дело обстоит так, что проблемы этих уровней берет на себя разработчик сложного приложения.

Над транспортным протоколом располагается уровень приложений. Этот уровень изначально включал виртуальный терминал – TELNET, протоколы FTP и SMTP. Позднее к ним добавились: служба доменных имен – DNS[30], отображающая логические имена хост-машин на их сетевые адреса, протокол для передачи новостей – NNTP[31], и протокол для работы с гипертекстовыми документами во Всемирной паутине – HTTP.

Практическая реализация стека TCP/IP

На рисунке 3 показаны уровни стека TCP/IP, имеющиеся в операци-

[29] UDP – User datagram protocol, протокол пользовательских датаграмм.

[30] DNS – Domain name system, доменная система имен.

[31] NNTP – Network news transfer protocol, сетевой протокол передачи новостей. Используется для распределения новостей по серверам и клиентам NNTP. Протокол обеспечивает хранение новостей в центральной базе данных сервера, индексацию, перекрестные ссылки и уничтожение сообщений после истечения определенного срока.

онной системе Windows XP. Уровни реализованы в виде программных модулей, которые можно добавлять или удалять в окне свойств настроенного соединения.

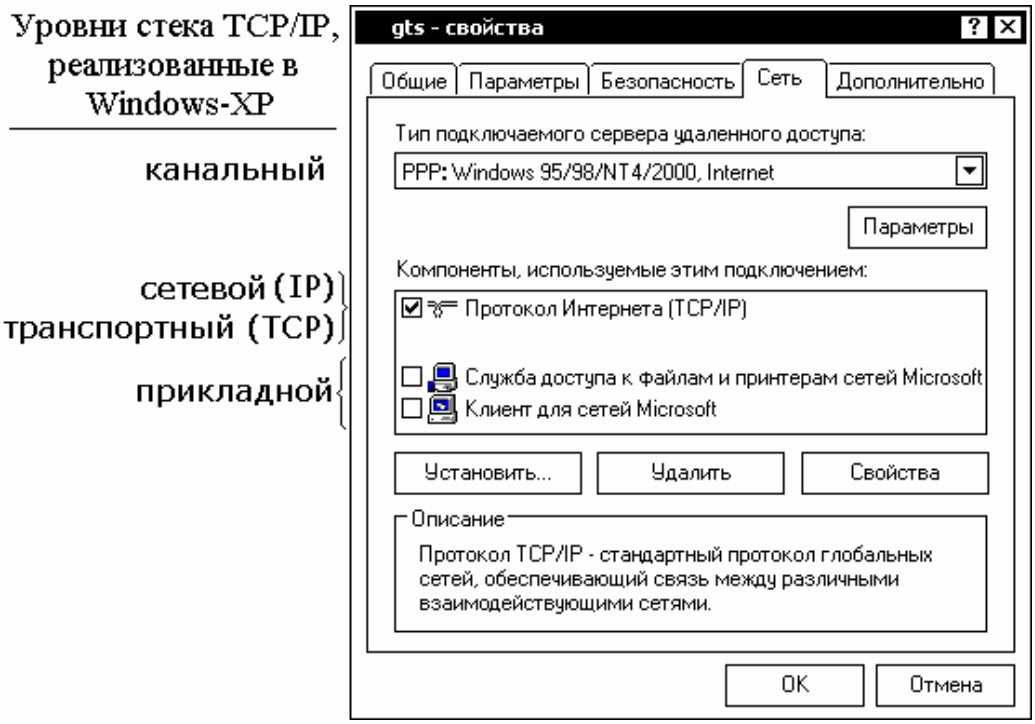


Рис. 3. Уровни стека TCP/IP в Windows XP.

Более подробно построение интернета на основе протоколов TCP/IP рассмотрено в главе 1.21.

1.5. Сравнение моделей OSI и TCP/IP

Обе модели имеют много общего. Они имеют многоуровневую иерархию, поддерживают понятие стека протоколов. Назначение уровней примерно одинаково. Все уровни от транспортного и ниже используют протоколы для поддержки взаимодействия типа точка–точка, не зависящего от организации сети. Все уровни выше транспортного ориентированы на приложения.

В модели OSI центральными являются три понятия. Они определяют методологическое значение модели своим четким выделением и разделением:

- сервис – определяет, что делает уровень, но не говорит как;
- интерфейс – определяет для вышележащего уровня доступ к сервису;
- протокол – определяет реализацию сервиса.

В TCP/IP модели нет столь четкого выделения аналогичных понятий. Этот факт есть следствие того, как создавались модели. Модель TCP/IP соз-

давалась *post factum*, а OSI *до того*, как появились протоколы. Понятие протокола в OSI абсолютно не зависит от остальных частей модели. Например, изначально протоколы канального уровня в OSI создавались для соединений точка–точка. Позднее, когда появились средства типа вещания, на этот уровень были добавлены соответствующие протоколы. Никаких других изменений не последовало.

Модель TCP/IP была создана, когда стек TCP/IP уже существовал и успешно работал. Поэтому модель прекрасно описывала этот стек, но только его и никакой другой.

Модели имеют разное число уровней. Обе имеют уровни приложений, транспортный и сетевой. Остальные уровни разные.

Модель OSI поддерживает на сетевом уровне как сервис с соединением, так и без соединения. На транспортном уровне поддерживается сервис только с соединением. В TCP/IP наоборот: сетевой уровень обеспечивает сервис без соединения, а транспортный – как с соединением, так и без.

Недостатки модели и протоколов OSI

Ни модель и протоколы ISO OSI, ни модель и протоколы TCP/IP не являются совершенными. В конце 80-х годов казалось, что у модели OSI нет конкурентов. Однако в настоящее время очевидно, что протоколы TCP/IP используются, мягко говоря, значительно шире. В чем причины? Начнем с недостатков модели и протоколов OSI.

Протоколы OSI были созданы не вовремя – введение стандарта должно следовать за окончанием исследований, но прежде чем начнутся крупные вложения в разработку. Протоколы OSI не технологичны:

- функции между семью уровнями распределены не равномерно;
- описание модели и ее протоколов очень сложно;
- некоторые функции (управление потоком, исправление ошибок, адресация) повторяются на каждом уровне;
- для некоторых функций не ясно, на какой уровень их поместить (виртуальный терминал); шифрование и защита отсутствуют;
- модель слишком ориентирована на сервис с соединениями и мало внимания уделяет сервису без соединений;
- протоколы OSI трудно реализуемы – первые реализации были громоздки и неэффективны.

Недостатки эталонной модели TCP/IP

Модель TCP/IP имеет следующие недостатки:

- нет четкого разграничения понятий сервис, интерфейс, протокол;
- модель годится только для описания стека TCP/IP;
- уровень хост–сеть по существу уровнем не является, это больше интерфейс;
- не разделяются физическая среда передачи и уровень канала данных;
- протоколы TCP и IP тщательно разработаны и эффективно реализованы, но этого нельзя сказать о многих других протоколах (протокол виртуального терминала, TELNET).

По существу, модель OSI доказала свою эффективность как методологический инструмент, чего нельзя сказать о протоколах. С TCP/IP все наоборот – модели по существу нет, зато протоколы получили широкое распространение.

1.6. Стандартные стеки коммуникационных протоколов

Все компоненты сети должны работать согласованно, для этого приняты многочисленные стандарты, обеспечивающие совместимость оборудования и программ различных фирм-изготовителей.

Важнейшим направлением стандартизации в области вычислительных сетей является стандартизация коммуникационных протоколов. В настоящее время в сетях используется большое количество стеков коммуникационных протоколов. Наиболее популярными являются стеки: TCP/IP, IPX/SPX, NetBIOS/SMB и OSI. Все они используют одни и те же хорошо стандартизованные протоколы Ethernet, Token Ring, FDDI и некоторые другие, позволяющие использовать в сетях одну и ту же аппаратуру. Зато на верхних уровнях стеки работают по собственным протоколам, которые часто не соответствуют иерархии, рекомендуемой моделью OSI. В частности, функции сеансового и представительного уровней, как правило, объединены с прикладным уровнем. Такое несоответствие как раз и связано с тем, что модель OSI появилась как результат обобщения уже существующих и реально используемых стеков, а не наоборот.

Стек OSI

Следует различать *модель OSI* и *стек OSI*. В то время как модель OSI является теоретической схемой взаимодействия открытых систем, стек OSI представляет собой набор вполне конкретных спецификаций. В отличие от других стеков протоколов, стек OSI полностью соответствует модели OSI. Он включает спецификации протоколов для всех семи уровней взаимодействия, определенных в модели. На нижних уровнях стек поддерживает Ethernet, Token Ring, FDDI, протоколы глобальных сетей, X.25 и ISDN, – то есть использует разработанные вне стека протоколы нижних уровней, как и все другие стеки. Протоколы сетевого, транспортного и сеансового уровней стека OSI специфицированы и реализованы различными производителями, но распространены мало. Наиболее популярными протоколами стека OSI являются прикладные протоколы. Например: протокол эмуляции терминала VTP, протоколы справочной службы X.500, электронной почты X.400 и ряд других.

Из-за своей сложности протоколы OSI требуют больших затрат вычислительной мощности центрального процессора, что делает их более подходящими для мощных машин, а не для сетей персональных компьютеров. На основе стека OSI реализуется взаимодействие в высокопроизводительных многомашинных вычислительных системах.

Стек TCP/IP

Стек TCP/IP был разработан для связи сети ARPANET с другими сетями как набор общих протоколов для разнородной вычислительной среды. Сегодня этот стек используется для связи между компьютерами интернета, 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[32], PPP, протоколы территориальных сетей X.25 и ISDN.

[32] SLIP – Serial line internet protocol, межсетевой протокол для последовательного канала. Устаревший протокол, обеспечивавший реализацию сетевых протоколов при соединении двух систем последовательными (телефонными) линиями. В настоящее время вместо SLIP в основном используется протокол PPP.

Основными протоколами стека, давшими ему название, являются протоколы TCP и IP. В терминологии модели OSI они относятся к транспортному и сетевому уровням соответственно. IP обеспечивает продвижение пакета по составной сети, а TCP гарантирует надежность его доставки.

За долгие годы использования 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, протокол эмуляции терминала TELNET, почтовые протоколы SMTP, POP3 и IMAP, используемые в электронной почте интернета, гипертекстовые сервисы службы WWW и многие другие.

Сегодня стек TCP/IP представляет собой один из самых распространенных стеков транспортных протоколов вычислительных сетей. Действительно, только в интернете объединено более 100 миллионов компьютеров по всему миру, активно взаимодействующих друг с другом с помощью стека протоколов TCP/IP.

Рост популярности интернета привел и к изменениям в расстановке сил в мире коммуникационных протоколов – протоколы TCP/IP, на которых построен интернет, значительно потеснили лидера прошлых лет – стек IPX/SPX компании Novell.

Хотя протоколы TCP/IP неразрывно связаны с интернетом, существует большое количество локальных, корпоративных и территориальных сетей, непосредственно не являющихся частями интернета, но также использующих протоколы TCP/IP. Чтобы отличать их от интернета, эти сети называют просто IP-сетями.

Поскольку стек TCP/IP изначально создавался для интернета, он имеет много особенностей, дающих ему преимущество перед другими протоколами, когда речь заходит о построении глобальных сетей. В частности, очень полезным свойством, делающим возможным применение протокола в больших сетях, является его способность фрагментировать пакеты. Действительно, большая сеть, как правило, состоит из более мелких сетей, построенных на совершенно разных принципах. В каждой из них может быть установлена собственная величина максимальной длины единицы передаваемых данных (кадра). В таком случае при переходе из одной сети, имеющей большую максимальную длину, в сеть с меньшей максимальной длиной может возникнуть необходимость деления передаваемого кадра на несколько частей. Протокол

IP стека TCP/IP эффективно решает эту задачу.

Другой особенностью стека TCP/IP является гибкая система адресации, позволяющая более просто по сравнению с другими протоколами аналогичного назначения включать в составную сеть сети других технологий. Это свойство также способствует применению стека TCP/IP для построения больших гетерогенных сетей.

Стек IPX/SPX

Этот стек является оригинальным стеком протоколов фирмы Novell, разработанным для сетевой операционной системы NetWare еще в начале 80-х годов. Протокол сетевого уровня IPX[33] и протокол сеансового уровня SPX[34] являются адаптацией протоколов XNS фирмы Xerox. Популярность стека IPX/SPX непосредственно связана с самой операционной системой Novell NetWare, которая долгое время сохраняла мировое лидерство по числу сетевых компьютеров, на которые была установлена. В последнее время ее роль значительно снизилась, уступив место лидера операционным системам Windows NT/2000/XP/Vista и различным реализациям UNIX (FreeBSD, Solaris, HP-UX, Linux и др.).

Многие особенности стека IPX/SPX обусловлены ориентацией ранних версий NetWare (до версии 4.0) на работу в локальных сетях небольших размеров, состоящих из персональных компьютеров со скромными ресурсами. Понятно, что для таких компьютеров нужны протоколы, на реализацию которых требуется минимальное количество оперативной памяти[35] и которые быстро работают на процессорах небольшой вычислительной мощности.

В результате ранние версии протоколов стека IPX/SPX хорошо работали в локальных сетях и не очень – в больших корпоративных сетях, так как они слишком перегружали медленные глобальные связи широковещательными пакетами, которые интенсивно использовались несколькими протоко-

[33] IPX – Internetwork packet exchange, межсетевой обмен пакетами.

[34] SPX – Sequenced packet exchange, последовательный обмен пакетами.

[35] Достаточно долгое время количество оперативной памяти в IBM-совместимых компьютерах ограничивалось объемом 640 Кбайт. Известно высказывание Билла Гейтса, датируемое 1982 годом: «Никому не понадобится больше 640 килобайт оперативной памяти на компьютере!» Развитие графического интерфейса и приложений, скорость работы которых значительно зависела от объема памяти, привело к существенному росту доступной и используемой оперативной памяти в настольных компьютерах и резкому снижению ее стоимости.

лами этого стека (например, для установления связи между клиентами и серверами). Это обстоятельство, а также тот факт, что стек IPX/SPX является собственностью фирмы Novell, и на его реализацию нужно получать лицензию, долгое время ограничивали распространенность его только сетями на основе NetWare.

Однако с момента выпуска версии NetWare 4.0 Novell внесла и продолжает вносить в протоколы серьезные изменения, направленные на их адаптацию для работы в корпоративных сетях. Сейчас стек IPX/ SPX реализован не только в NetWare, но и в нескольких других популярных сетевых ОС, например SCO UNIX, Sun Solaris, Microsoft Windows.

Стек NetBIOS/SMB

Этот стек широко используется в продуктах компаний IBM[36] и Microsoft. На физическом и канальном уровнях этого стека используются все наиболее распространенные протоколы Ethernet, Token Ring, FDDI и другие. На верхних уровнях работают протоколы NetBEUI и SMB.

Протокол NetBIOS[37] появился в 1984 году как сетевое расширение стандартных функций базовой системы ввода/вывода (BIOS) IBM PC для сетевой программы PC Network фирмы IBM. В дальнейшем он был заменен так называемым протоколом расширенного пользовательского интерфейса NetBEUI[38]. Для обеспечения совместимости приложений в качестве интерфейса к протоколу NetBEUI был сохранен интерфейс NetBIOS. Протокол NetBEUI разрабатывался как эффективный протокол, потребляющий немного ресурсов и предназначенный для сетей, насчитывающих не более 200 рабочих станций.

В протоколе содержится много полезных сетевых функций, которые можно отнести к сетевому, транспортному и сеансовому уровням модели OSI,

[36] IBM – International business machines, образована в 1911 году слиянием трех крупных компаний, первоначально называлась CTR (Computing-Tabulating-Recording). Название IBM получила в 1924 году. Крупнейшая мировая корпорация, занимающаяся разработками в области информационных технологий. В числе ее разработок – цифровой программируемый компьютер на электромагнитных реле, диодный лазер (основа оптических запоминающих устройств), гибкие магнитные диски, накопители на жестких магнитных дисках, первый язык программирования высокого уровня FORTRAN, а также персональный компьютер.

[37] NetBIOS – Network basic input/output system, сетевая базовая система ввода-вывода.

[38] NetBEUI – NetBIOS extended user interface, расширенный пользовательский интерфейс NetBIOS.

однако с его помощью невозможна маршрутизация пакетов. Это ограничивает применение протокола NetBEUI локальными сетями, не разделенными на подсети, и делает невозможным его использование в составных сетях.

Протокол SMB[39] выполняет функции сеансового, представительного и прикладного уровней. На основе SMB реализуется файловая служба, а также службы печати и передачи сообщений между приложениями.

На рис. 4 показано соответствие некоторых, наиболее популярных протоколов уровням модели OSI. В большинстве случаев разработчики стеков отдавали предпочтение скорости работы сети в ущерб модульности – ни один стек, кроме стека OSI, не разбит на семь уровней. Чаще всего в стеке явно выделяются 3-4 уровня: уровень сетевых адаптеров, реализующий протоколы физического и канального уровней, сетевой уровень, транспортный уровень и уровень служб, объединяющий функции сеансового, представительного и прикладного уровней.

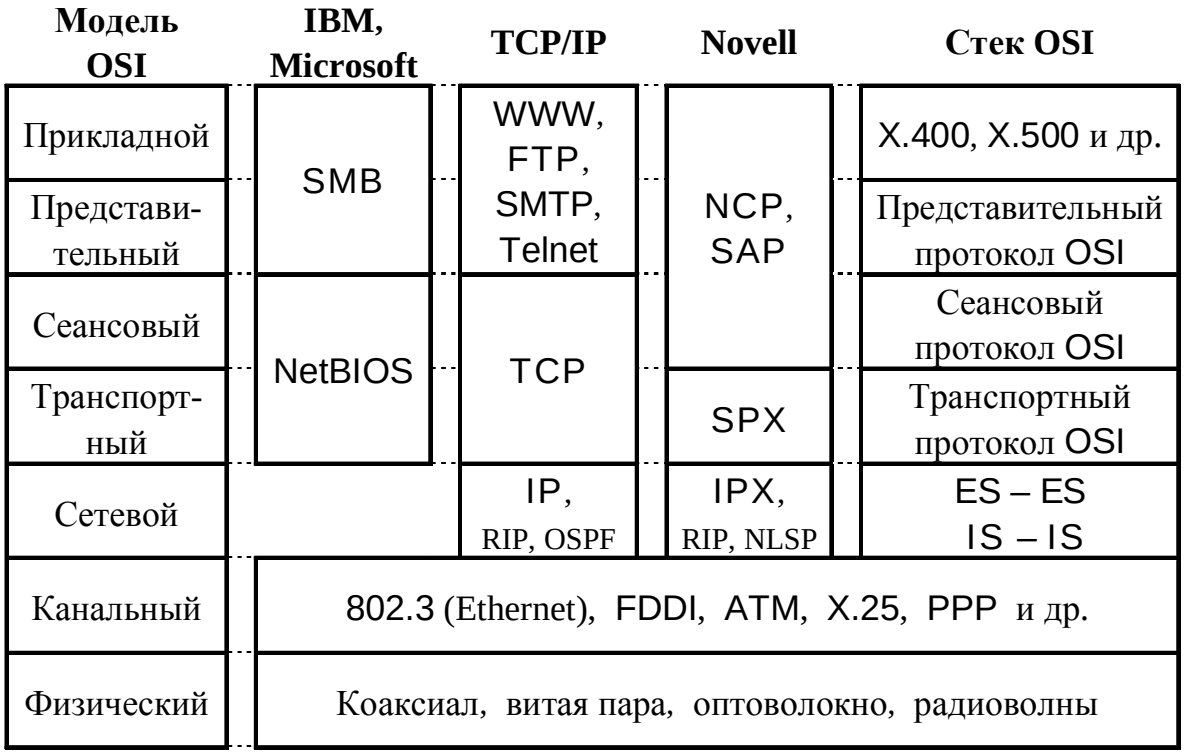


Рис. 4. Соответствие популярных стеков протоколов модели OSI

[39] SMB – Server message block, блочные сообщения сервера. Формат сообщений на основе протокола совместного использования файлов Microsoft/3Com, используемый для передачи простых файловых запросов (open – открыть, close – закрыть, read – прочитать, write – записать и т. п.) между клиентами и серверами.

1.7. Стандарты IEEE 802

В 1980 году в институте IEEE[40] был образован комитет 802 по стандартизации ЛВС, в результате работы которого принято семейство стандартов IEEE 802.x, содержащих рекомендации по проектированию нижних уровней локальных сетей. Позже результаты работы комитета легли в основу комплекса международных стандартов ISO 8802-1...5, созданных на основе распространенных фирменных стандартов сетей Ethernet, ArcNet и Token Ring.

Стандарты семейства IEEE 802.x охватывают только два нижних уровня семиуровневой модели OSI – физический и канальный (рис. 5). Это связано с тем, что именно они в наибольшей степени отражают специфику локальных сетей. Старшие же уровни, начиная с сетевого, в значительной степени имеют общие черты как для локальных, так и для глобальных сетей.

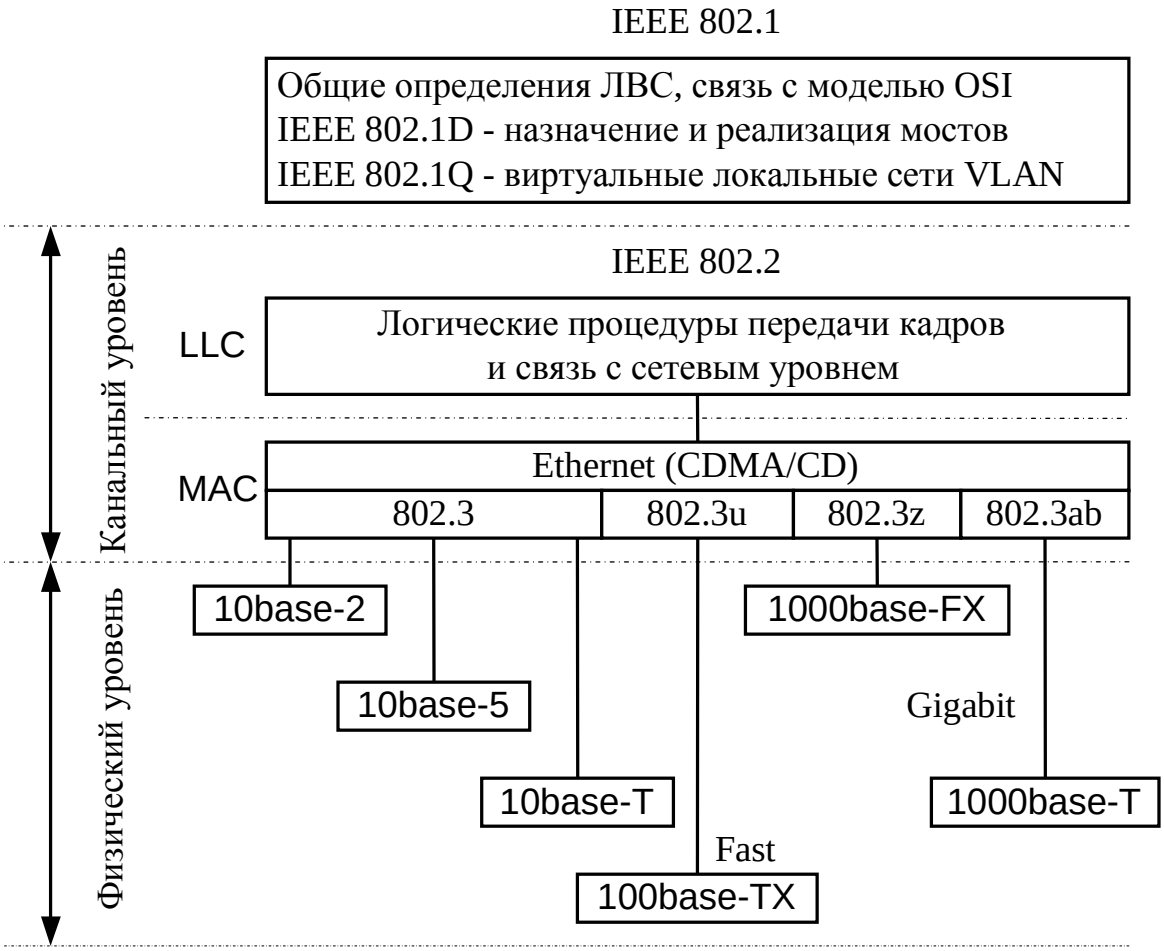


Рис. 5. Структура стандартов IEEE 802.x для технологии Ethernet.

[40] IEEE – Institute of electrical and electronics engineers, Институт специалистов по электричеству и электронике.

Стандарты 802.1 носят общий для всех технологий характер. В подкомитете 802.1 были разработаны общие определения локальных сетей и их свойств, определена связь трех уровней модели IEEE 802 с моделью OSI. Но наиболее практически важными являются стандарты 802.1, описывающие взаимодействие между собой различных технологий, а также построение более сложных сетей на основе базовых топологий. Эта группа стандартов носит общее название стандартов межсетевого взаимодействия (internetworking). Сюда входят стандарт 802.1d, описывающий логику работы моста/коммутатора, стандарт 802.1h, определяющий работу транслирующего моста, способного без маршрутизатора объединять сети Ethernet и FDDI, Ethernet и Token Ring и т. п. Набор стандартов, разработанных подкомитетом 802.1, постоянно растет.

Стандарты обычно разрабатываются не одной компанией, а группой заинтересованных компаний, после чего передаются в соответствующий подкомитет IEEE 802 для утверждения. Сегодня комитет 802 включает следующие подкомитеты:

- 802.1 – объединение сетей (internetworking);
- 802.1d – назначение и реализация мостов;
- 802.1h – спецификации транслирующего моста;
- 802.2 – управление логической передачей данных (Logical Link Control, LLC);
- 802.3 – Ethernet с методом доступа CSMA/CD (1985 г.);
- 802.3u – Fast Ethernet (1995 г.);
- 802.3z – Gigabit Ethernet (1998-1999 г.);
- 802.4 – локальные сети с методом доступа Token Bus (маркерная шина), использовались в промышленных сетях, в настоящее время не действует;
- 802.5 – локальные сети с методом доступа Token Ring (маркерное кольцо), разработка IBM;
- 802.6 – сети мегаполисов;
- 802.7 – техническая консультационная группа по широкополосной передаче (Broadband technical advisory group), не действует;
- 802.8 – техническая консультационная группа по волоконно-оптическим сетям (Fiber optic technical advisory group), не действует;
- 802.9 – интегрированные сети передачи голоса и данных для приложений реального времени (Integrated voice and data networks), не действует;

- 802.10 – виртуальные ЛВС и защита информации (Network security), не действует;
- 802.11 – беспроводные сети (Wireless networks). Подкомитеты:
  - 802.11a – полоса пропускания до 6,5 Мбит/с;
  - 802.11b (Wi-Fi – Wireless Fidelity), полоса пропускания до 11 Мбит/с;
  - 802.11g – полоса пропускания до 54 Мбит/с, радиус действия до 500 м на открытой местности;
  - 802.11n – до 200 Мбит/с, радиус действия до 2 км на открытой местности (еще даже не внедренный стандарт уже вытесняется более совершенным 802.16);
- 802.12 – локальные сети с методом доступа по требованию с приоритетами (Demand priority access LAN), были приняты для сетей технологии AnyLAN фирмы Hewlett-Packard, в настоящее время не действует;
- 802.13 – нет стандарта[41];
- 802.14 – кабельные модемы (рабочая группа распалась, поскольку в области кабельных модемов ее опередил промышленный консорциум);
- 802.15 – персональные сети, в том числе реализуемые посредством беспроводных соединений через Bluetooth[42];

---

[41] Человеческая психика устроена так, что ей для развития необходимы разнообразные стимулы, среди которых немаловажным является мистический аспект. В европейской традиции число 13 считается «несчастливым», чертовым числом, в силу чего многие тринадцатые объекты отсутствуют как таковые. Например, в респектабельных гостиницах США после двенадцатого этажа сразу идет четырнадцатый. В восточной традиции несчастливым считается цифра 4, и поэтому в домах отсутствует четвертый этаж, стараются не наступать на четвертую ступеньку лестницы и т.д. Русский обычай дарить нечетное количество цветов в букете по радостным событиям и приносить нечетное в похоронных венках и букетах – того же плана.

Как ни странно, но наиболее просвещенные в техническом плане специалисты порой оказываются не менее подвержены суевериям, нежели темные крестьяне XVIII века. Например, в комитете 802 так и не решились дать наименование «802.13» какому-либо из новых стандартов.

[42] Само слово Bluetooth можно перевести как «голубой зуб» или «голубая челюсть». Это, конечно, никоим образом не описывает ни сути технологии, ни чего-то еще. В 908 году у ютландского короля Горма Старого родился сын Харальд. Харальд I Блаатанд (в поздней транскрипции – Bluetooth, Синезубый – прозвище свое он получил из-за потемневшего переднего зуба), подчинил своей воле разрозненных викингов, объединил Данию с Южной Норвегией и Южной Швецией и создал единое Датское Королевство. Он же способствовал распространению в Скандинавии христианства, что бесспорно послужило единению культур.

Спустя тысячу лет, в феврале 1998 года компании Ericsson (Швеция), IBM (США),

- 802.16 – стандартизация радиоинтерфейсов и дополнительных функций, необходимых для организации беспроводной «последней мили». Коммерческое название — WiMAX[43]. Полоса пропускания до 70 Мбит/с, радиус действия до 50 км. Подкомитеты:
  - 802.16.1 – определяет радиоинтерфейс для систем, работающих на частотах от 10 до 66 ГГц;
  - 802.16.2 – регламентирует вопросы совместимости разных систем широкополосного беспроводного доступа;
  - 802.16.3 – определяет радиоинтерфейс для систем, работающих в лицензируемых диапазонах от 2 до 11 ГГц;
- 802.17 – гибкая технология пакетного кольца.

1.8. Сетевая технология Ethernet

Сетевая технология – это согласованный набор стандартных протоколов и реализующих их программно-аппаратных средств (сетевых адаптеров, драйверов, кабелей и разъемов), достаточный для построения вычислительной сети.

Стандарт Ethernet был принят в 1980 году. Число сетей, построенных на основе этой технологии, к настоящему моменту оценивается в несколько миллионов, а количество компьютеров, работающих в таких сетях, – в несколько сотен миллионов.

Принцип, положенный в основу Ethernet, – *случайный метод доступа* к разделяемой среде передачи данных. В качестве такой среды может использоваться толстый или тонкий коаксиальный кабель, витая пара, оптоволокно или радиоволны.

В технологии Ethernet компьютеры подключаются к разделяемой среде в соответствии с типовой структурой «общая шина». С помощью разделяе-

---

Intel (США), Toshiba (Япония) и Nokia (Финляндия) объединили свои усилия для создания технологии беспроводного соединения мобильных устройств. Прозвище короля Харальда I – Bluetooth – вновь стало символом объединения. Видимо, свою роль сыграло и то, что основы технологии были еще в 1994 году проработаны шведской компанией Ericsson. Логотип Bluetooth составляют руны, обозначающие инициалы короля.

Спецификация Bluetooth описывает пакетный способ передачи информации с временным мультиплексированием. Радиообмен происходит в полосе частот 2400-2483,5 МГц.

[43] Worldwide interoperability for microwave access, общее взаимодействие сетей микроволнового доступа.

мой во времени шины любые два компьютера могут обмениваться данными. Управление доступом к линии связи осуществляется специальными контроллерами – сетевыми адаптерами Ethernet. Каждый сетевой адаптер имеет уникальный адрес. Передача данных происходит со скоростью 10 Мбит/с. Эта величина является пропускной способностью сети Ethernet.

Суть случайного метода доступа состоит в следующем. Компьютер в сети Ethernet может передавать данные по сети, только если сеть свободна, то есть, если никакой другой компьютер в данный момент не занимается обменом. Поэтому важной частью технологии Ethernet является процедура определения доступности среды.

После того как компьютер убедился, что сеть свободна, он начинает передачу, при этом «захватывает» среду. Время монопольного использования разделяемой среды одним узлом ограничивается временем передачи одного кадра. *Кадр* – это единица данных, которыми обмениваются компьютеры в сети Ethernet. Кадр имеет фиксированный формат и наряду с полем данных содержит различную служебную информацию, например адрес получателя и адрес отправителя.

Сеть Ethernet устроена так, что при попадании кадра в разделяемую среду передачи данных все сетевые адаптеры одновременно начинают принимать этот кадр. Они анализируют адрес назначения, располагающийся в служебном поле кадра и, если этот адрес совпадает с их собственным адресом, кадр помещается во внутренний буфер сетевого адаптера. Таким образом компьютер-адресат получает предназначенные ему данные.

Иногда возникает ситуация, когда одновременно два или более компьютеров решают, что сеть свободна, и начинают передавать информацию. Такая ситуация называется *коллизией* и препятствует правильной передаче данных по сети. Вероятность возникновения коллизии зависит от интенсивности сетевого трафика. В стандарте Ethernet предусмотрен алгоритм обнаружения и корректной обработки коллизий.

После обнаружения коллизии сетевые адаптеры, которые пытались передать свои кадры, прекращают передачу и после паузы *случайной длительности* пытаются снова получить доступ к среде и передать тот кадр, который вызвал коллизию.

1.9. Методы коммутации

Нереально предоставить каждой паре взаимодействующих абонентов собственную прямую физическую линию связи, которой они могли бы монопольно владеть в течение длительного времени. Поэтому в любой сети всегда применяется какой-либо способ *коммутации*[44] абонентов, который обеспечивает доступность имеющихся физических каналов одновременно для нескольких абонентов сети.

Коммутация осуществляется при помощи устройств, называемых *коммутаторами*. Абоненты соединяются с ними линиями связи, каждая из которых используется в любой момент времени только одним абонентом. А уже линии связи между коммутаторами используются совместно (разделяются) несколькими абонентами.

Существуют три схемы коммутации потоков данных в среде передачи данных: *коммутация каналов*, *коммутация пакетов* и *коммутация сообщений*.

На рис. 6 приведена классификация методов коммутации.

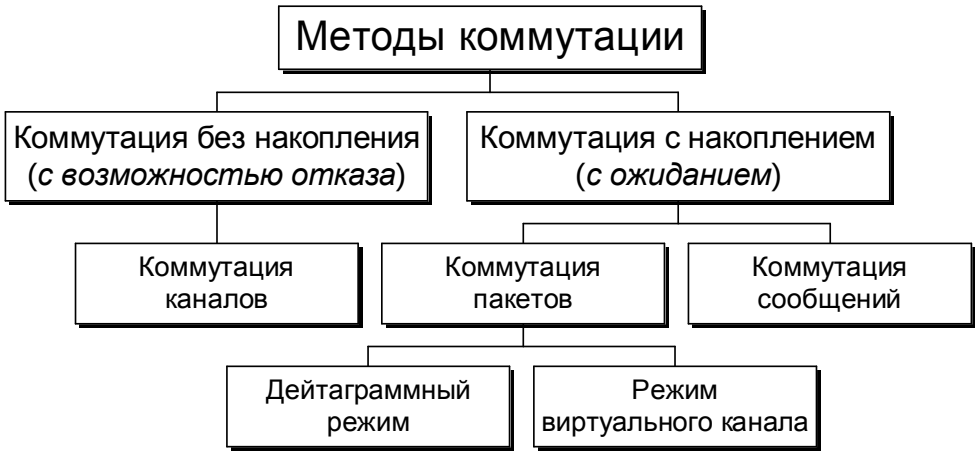


Рис. 6. Классификация методов коммутации в системах передачи данных.

Возможности и свойства этих схемы различны. Сети с коммутацией каналов ведут свое происхождение от первых телефонных сетей и имеют богатую историю. Сети с коммутацией сообщений послужили прототипом современных сетей с коммутацией пакетов, но сегодня в чистом виде практически не существуют. Последние 30 лет получили развитие сети с коммутацией пакетов.

[44] Коммутация – технология выбора направления передачи данных в сетях с маршрутизацией данных. Конкретные методы коммутации определяются поставленными задачами и стеком протоколов области взаимодействия открытых систем.

Кроме способов, различают виды коммутации. Обычно рассматривают два вида:

- *оперативная (динамическая) коммутация*, или *связь с установлением соединения*, при которой сеть разрешает установить соединение по инициативе пользователя. Коммутация выполняется на время сеанса связи, а затем связь разрывается. В общем случае любой пользователь сети может соединиться с любым другим пользователем сети. Обычно период соединения между парой пользователей составляет от нескольких секунд до нескольких часов и завершается при выполнении определенной работы. Примеры таких сетей – телефонные сети общего пользования, локальные сети, сети TCP/IP;
- *кроссовая (долговременная или постоянная) коммутация*, или *связь без установления соединения*[45], при которой сеть не предоставляет пользователю возможность выполнить динамическую коммутацию с другим произвольным пользователем сети. Вместо этого пара пользователей заказывает соединение на длительный период времени. Соединение устанавливается не пользователями, а персоналом, обслуживающим сеть. Время, на которое устанавливается постоянная коммутация, измеряется обычно несколькими месяцами. Режим постоянной коммутации в сетях с коммутацией каналов часто называется сервисом выделенных (dedicated) или арендуемых (leased) каналов. Наиболее популярными сетями, работающими в таком режиме, являются сети SDH, на основе которых строятся выделенные каналы связи с пропускной способностью в несколько гигабит в секунду.

Некоторые типы сетей поддерживают оба режима работы. Например, сети X.25 и ATM предоставляют возможность динамической связи с любым другим пользователем сети и в то же время отправки данных по постоянному соединению одному вполне определенному абоненту.

1.10. Коммутация каналов

Коммутация каналов подразумевает образование непрерывного составного физического канала из последовательно соединенных отдельных

[45] Это не значит, что соединение осуществляется по воздуху или телепатически. Суть в том, что при связи с установлением соединения соединение устанавливается при каждом сеансе, а при связи без установления соединения соединение устанавливается один раз на длительный период времени, в течение которого может быть несколько аналогичных сеансов работы.

канальных участков для прямой передачи данных между узлами. Отдельные каналы соединяются между собой специальной аппаратурой – коммутаторами, которые могут устанавливать связи между любыми конечными узлами сети. В сети с коммутацией каналов перед передачей данных всегда необходимо выполнить процедуру установления соединения, в процессе которой и создается составной канал.

Коммутаторы, а также соединяющие их каналы должны обеспечивать одновременную передачу данных нескольких абонентских каналов. Для этого они должны быть высокоскоростными и поддерживать какую-либо технику совместного разделения каналов. В настоящее время для мультиплексирования абонентских каналов используются две техники:

- *аналоговая*, или техника частотного мультиплексирования;
- *цифровая*, или техника мультиплексирования с разделением времени.

Метод частотного мультиплексирования

Частотное мультиплексирование каналов[46] было разработано для телефонных сетей, но применяется и для других видов, например сетей кабельного телевидения. Рассмотрим особенности этого вида мультиплексирования на примере телефонной сети.

Для качественной передачи речи достаточно образовать между двумя абонентами канал с полосой пропускания в 3100 Гц. Полоса пропускания кабельных систем с промежуточными усилителями, соединяющими телефонные коммутаторы между собой, обычно составляет сотни килогерц и мегагерц.

Для разделения абонентских каналов применяют технику модуляции высокочастотного несущего сигнала низкочастотным речевым сигналом. Абонентские каналы образуют *каналы тональной частоты* (ТЧ). Спектр сигнала каждого абонентского канала переносится коммутатором в собственный диапазон частот, и в одном *широкополосном аналоговом канале* между коммутаторами возможно одновременно передавать сигналы нескольких каналов ТЧ (рис. 7). Такой канал называют *уплотненным*.

Выходной FDM-коммутатор выделяет модулированные сигналы каждой несущей частоты и передает их на соответствующий выходной канал, к которому непосредственно подключен абонентский телефон.

[46] FDM – Frequency division multiplexing.

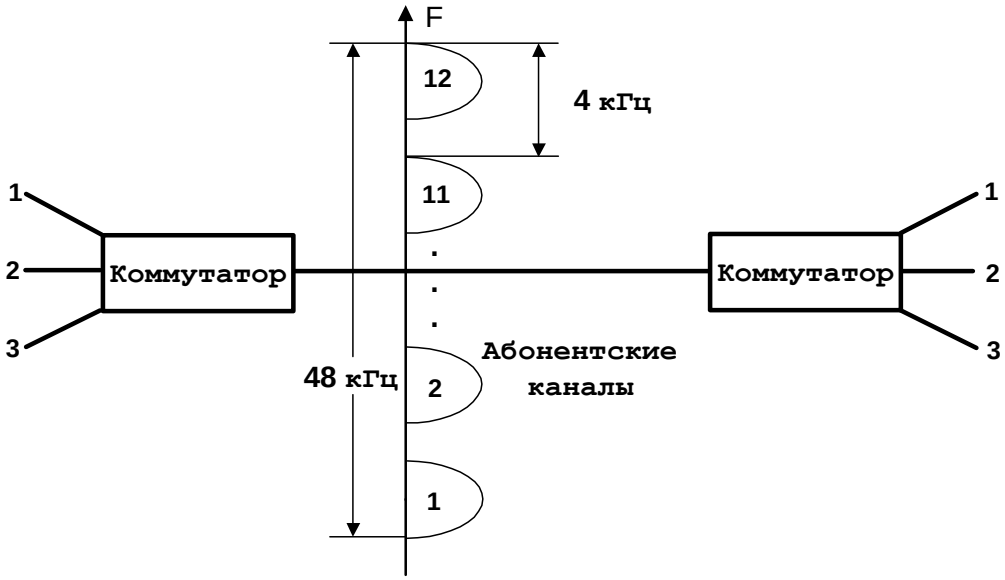


Рис. 7. Базовая группа каналов тональной частоты

Принцип частотной коммутации остается неизменным и в сетях других видов, меняются только границы полос, выделяемых отдельному абонентскому каналу, и количество низкоскоростных каналов в уплотненном высокоскоростном.

Коммутация каналов на основе разделения времени

Коммутация на основе техники разделения частот[47] разрабатывалась в расчете на передачу непрерывных сигналов. При переходе к цифровой форме была разработана техника мультиплексирования, ориентированная на дискретный характер передаваемых данных.

Аппаратура TDM-сетей – мультиплексоры, коммутаторы, демультиплексоры – работает в режиме разделения времени. Они поочередно обслуживают все абонентские каналы в циклическом режиме. Цикл работы оборудования TDM равен 125 мкс. Мультиплексор или коммутатор успевает вовремя обслужить любой абонентский канал и передать его очередной замер далее по сети. Каждому соединению выделяется один *квант времени* цикла работы аппаратуры, называемый также *тайм-слотом*. Длительность тайм-слота зависит от числа абонентских каналов, обслуживаемых мультиплексором или коммутатором.

[47] TDM – Time division multiplexing. Реже используется другое название – техника синхронного режима передачи (STM, Synchronous transfer mode). В беспроводных сетях мобильной связи используется родственная технология TDMA (DAMPS).

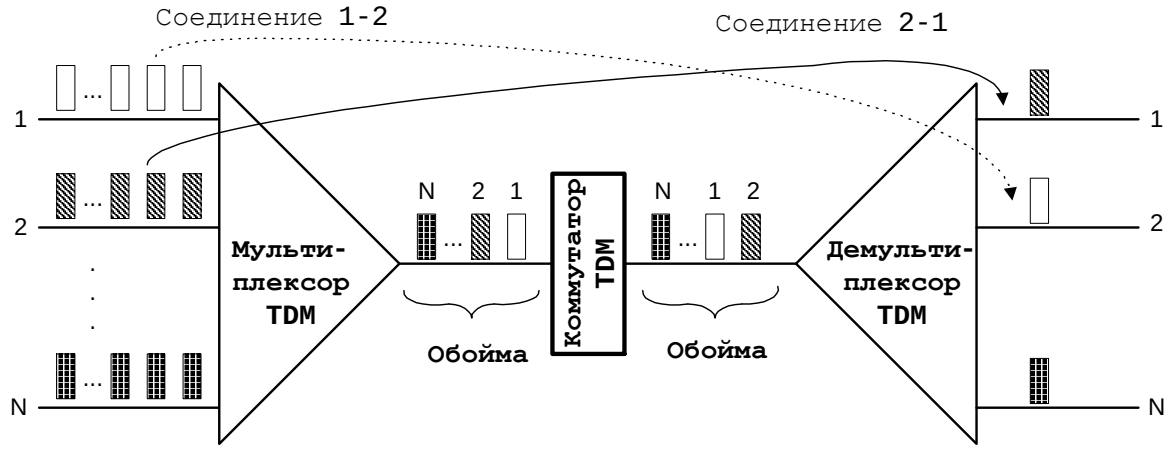


Рис. 8. Коммутация на основе разделения канала во времени

Мультиплексор TDM принимает информацию по N входным каналам от конечных абонентов, каждый из которых передает данные по абонентскому каналу со скоростью 64 Кбит/с (1 байт каждые 125 мкс). В каждом цикле мультиплексор выполняет следующие действия:

- прием от каждого канала очередного байта данных;
- составление из принятых байтов *уплотненного кадра*, называемого также *обоймой*;
- передача уплотненного кадра на выходной канал с битовой скоростью, равной N×64 Кбит/с, где N – количество тайм-слотов, выделенных для данного устройства.

Демультиплексор выполняет обратную задачу – разбирает байты уплотненного кадра и распределяет их по выходным каналам, при этом порядковый номер байта в обойме соответствует номеру выходного канала.

Коммутатор принимает уплотненный кадр по скоростному каналу от мультиплексора и записывает каждый байт из него в отдельную ячейку буферной памяти, причем в том порядке, в котором эти байты были упакованы в уплотненный кадр. Для выполнения операции коммутации байты извлекаются из буферной памяти не в порядке поступления, а в таком порядке, который соответствует поддерживаемым в сети соединениям абонентов.

Соединение в сети TDM всегда обладает известной и фиксированной пропускной способностью, кратной 64 Кбит/с.

Сети, использующие технику TDM, требуют синхронной работы всего оборудования, что и определило второе название этой техники – синхронный режим передачи. Нарушение синхронности разрушает требуемую коммутацию абонентов.

Сети TDM могут поддерживать режим динамической коммутации и режим постоянной коммутации, а иногда и оба сразу. Например, основным режимом цифровых телефонных сетей, работающих на основе технологии TDM, является динамическая коммутация, но они поддерживают также и постоянную коммутацию, предоставляя абонентам службу выделенных каналов.

Сегодня практически все данные – голос, изображение, файлы – передаются в цифровой форме. Поэтому выделенные каналы TDM-технологии, обеспечивающие нижний уровень для передачи цифровых данных, являются универсальными каналами для построения сетей любого типа: телефонных, телевизионных и компьютерных.

Общие свойства сетей с коммутацией каналов

Сети с коммутацией каналов обладают несколькими важными общими свойствами независимо от того, какой тип мультиплексирования в них используется.

Сети с динамической коммутацией требуют предварительной процедуры установления соединения между абонентами. Для этого в сеть передается адрес вызываемого абонента, проходящий через коммутаторы и настраивающий их на последующую передачу данных. Запрос на установление соединения маршрутизируется от одного коммутатора к другому и достигает вызываемого абонента. Сеть может отказать в установлении соединения в случаях:

- *если занят коммутатор*, то есть исчерпана емкость требуемого выходного канала. Для FDM-коммутатора емкость выходного канала равна количеству частотных полос этого канала, для TDM-коммутатора – количеству тайм-слотов, на которые делится цикл работы канала;
- *если занят абонент*, то есть запрашиваемый абонент уже установил с кем-нибудь соединение.

Возможность отказа в соединении является недостатком метода коммутации каналов.

Еще одним недостатком сетей с коммутацией каналов является *невозможность применения пользовательской аппаратуры*, работающей с разной скоростью. Отдельные части составного канала должны работать с одинаковой скоростью, так как сети с коммутацией каналов не буферизуют данные.

Если соединение может быть установлено, то ему выделяется фиксированная полоса частот в FDM-сетях или фиксированная пропускная способность в TDM-сетях. Эти величины остаются неизменными в течение всего периода соединения. Гарантированная пропускная способность сети после установления соединения является важным свойством, необходимым для *приложений реального времени*, таких как передача голоса, изображения или удаленное управление объектами. Однако динамически изменять пропускную способность канала по требованию абонента сети с коммутацией каналов не могут, что делает их неэффективными в условиях *пульсирующего трафика* (нагрузки на сеть).

Сети с коммутацией каналов хорошо приспособлены для потоков данных постоянной скорости, когда единицей коммутации является не отдельный байт или пакет данных, а долговременный синхронный поток данных между абонентами.

Дуплексный режим работы на базе технологий FDM, TDM и WDM

В зависимости от направления передачи данных способы передачи данных по линии связи делятся на следующие типы:

- *симплексный* – передача осуществляется только в одном направлении;
- *полудуплексный* – передача ведется попеременно в обоих направлениях;
- *дуплексный* – передача ведется одновременно в двух направлениях.

Полудуплексный режим используется при наличии единственного физического канала. Примером такой передачи служит технология Ethernet.

Дуплексный режим – наиболее универсальный и производительный способ работы канала. Самым простым вариантом организации дуплексного режима является использование двух независимых физических каналов (двух пар проводников или двух световодов) в кабеле, каждый из которых работает в симплексном режиме, то есть передает данные в одном направлении. Эта технология лежит в основе реализации дуплексного режима работы во многих сетевых технологиях, например Fast Ethernet или ATM. В случае единственного физического канала можно организовать дуплексный режим работы разделением канала на два логических подканала с помощью техники FDM или TDM.

Дуплексный режим работы в волоконно-оптических кабелях (при использовании одного оптического волокна) можно реализовать также переда-

чей данных в одном направлении с помощью светового пучка одной длины волны, а в обратном – другой длины волны. Такая техника относится к методу FDM, однако для оптических кабелей она получила название *разделения по длине волны*[48].

Глобальные сети с коммутацией каналов

Для построения глобальных связей в корпоративной сети доступны сети с коммутацией каналов двух типов – традиционные аналоговые телефонные сети и цифровые сети с интеграцией услуг ISDN. Достоинством сетей с коммутацией каналов является их распространенность, что характерно особенно для аналоговых телефонных сетей.

Недостатком аналоговых телефонных сетей является низкое качество составного канала, которое объясняется широким использованием аналоговых телефонных коммутаторов. Они сильно подвержены воздействию помех (например, грозовых разрядов), которые трудно отличить от полезного сигнала. Кроме качества каналов, аналоговые сети также характеризуются большим временем установления соединения.

Сети с интегральными услугами

ISDN[49] относятся к сетям, в которых основным режимом коммутации является режим коммутации каналов, а данные обрабатываются в цифровой форме. Архитектура сети ISDN предусматривает несколько видов служб, показанных на рис. 9:

- некоммутируемые средства (выделенные цифровые каналы);
- коммутируемая телефонная сеть общего пользования;
- сеть передачи данных с коммутацией каналов;
- сеть передачи данных с коммутацией пакетов;
- сеть передачи данных с трансляцией кадров (*frame relay*);
- средства контроля и управления работой сети.

Как видно из приведенного списка, транспортные службы сетей ISDN покрывают очень широкий спектр услуг. Большое внимание уделено средствам контроля сети, позволяющим маршрутизировать вызовы для установления соединения, а также осуществлять мониторинг и управление сетью.

[48] WDM – Wave division multiplexing.
[49] ISDN – Integrated services digital network, цифровые сети с интегральными услугами.

Управляемость сети обеспечивается интеллектуальностью коммутаторов и конечных узлов сети, поддерживающих стек протоколов, в том числе и специальных протоколов управления.

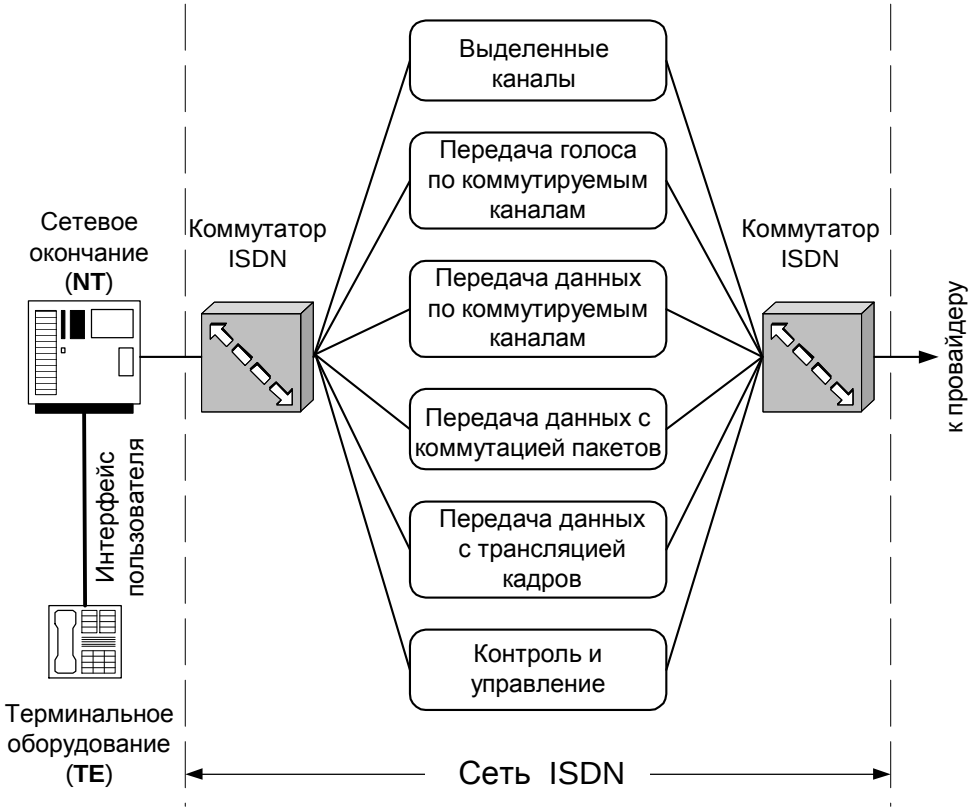


Рис. 9. Службы ISDN.

Стандарты ISDN описывают ряд услуг прикладного уровня: факсимильную связь на скорости 64 Кбит/с, телексную связь на скорости 9600 бит/с, видеотекс на скорости 9600 бит/с и некоторые другие.

На практике не все сети ISDN поддерживают все стандартные службы. Служба *frame relay*, хотя и была разработана в рамках сети ISDN, реализуется обычно с помощью отдельной сети коммутаторов кадров, не пересекающейся с сетью коммутаторов ISDN.

Базовой скоростью сети ISDN является скорость канала DS-0, то есть 64 Кбит/с. Эта скорость ориентируется на самый простой метод кодирования голоса – PCM[50], хотя дифференциальное кодирование и позволяет передавать

[50] PCM – Pulse code modulation, импульсно-кодовая модуляция. Используется для оцифровки аналоговых сигналов перед их передачей. Для получения ИКМ-модулированного сигнала амплитуда аналогового сигнала измеряется через равные промежутки времени. Мгновенное измеренное значение аналогового сигнала округляется до ближайшего из нескольких заранее определенных значений. Этот процесс называется квантованием, а количество уровней всегда берется кратным степени двойки. Таким обра-

голос с тем же качеством на скорости 32 или 16 Кбит/с.

Одним из базовых принципов ISDN является предоставление пользователю стандартного интерфейса, с помощью которого пользователь может запрашивать у сети разнообразные услуги. Этот интерфейс образуется между двумя типами оборудования, устанавливаемого в помещении пользователя: терминальным оборудованием пользователя TE (компьютер с соответствующим адаптером, маршрутизатор, телефонный аппарат) и сетевым окончанием NT, которое представляет собой устройство, завершающее канал связи с ближайшим коммутатором ISDN.

Пользовательский интерфейс основан на каналах трех типов:

- **B** со скоростью передачи данных 64 Кбит/с;
- **D** со скоростью передачи данных 16 или 64 Кбит/с;
- **H** со скоростью передачи данных 384 Кбит/с (H0), 1536 Кбит/с (H11) или 1920 Кбит/с (H12).

Каналы типа **B** обеспечивают передачу пользовательских данных (оцифрованного голоса, компьютерных данных или смеси голоса и данных) и с более низкими скоростями, чем 64 Кбит/с. Разделение данных выполняется с помощью техники TDM. Разделением канала **B** на подканалы в этом случае должно заниматься пользовательское оборудование, сеть ISDN всегда коммутирует целые **B**-каналы.

Канал типа **D** выполняет две основные функции. Первой и основной является передача адресной информации, на основе которой осуществляется коммутация каналов типа **B**. Второй функцией является поддержание услуг низкоскоростной сети с коммутацией пакетов для пользовательских данных. Обычно эта услуга выполняется сетью в то время, когда каналы типа **D** свободны от выполнения основной функции.

Каналы типа **H** предоставляют пользователям возможности высокоскоростной передачи данных.

Пользовательский интерфейс ISDN представляет собой набор каналов определенного типа и с определенными скоростями. Оборудование пользователя подключается к ISDN через DSL[51]. Длина двухпроводного DSL – до 5,5 км.

зом, на выходе модулятора получается набор битов (0 или 1). На приемном конце канала связи демодулятор преобразует последовательность битов в импульсы с тем же уровнем квантования, который использовал модулятор. Далее эти импульсы используются для восстановления аналогового сигнала.

[51] DSL – Digital subscriber line, цифровая абонентская линия.

Сети ISDN свободны от многих недостатков аналоговых сетей. Они предоставляют пользователям высококачественные линии связи, а время установления соединения в сетях ISDN существенно меньше.

Однако даже при качественных каналах связи, которые могут обеспечить сети с коммутацией каналов, для построения корпоративных глобальных связей эти сети могут оказаться экономически неэффективными. В таких сетях пользователи платят не за объем переданного трафика, а за время соединения, что при трафике с большими пульсациями не выгодно.

1.11. Коммутация сообщений

Под *коммутацией сообщений* понимается передача единого блока данных между транзитными компьютерами сети с временной буферизацией этого блока на каждом компьютере.

Коммутация сообщений предназначена для организации взаимодействия пользователей в режиме *off-line*[52], когда не ожидается немедленной реакции на сообщение. Сообщение, в отличие от пакета, имеет произвольную длину, которая определяется не технологическими соображениями, а содержанием. Например, сообщением может быть текстовый документ, файл с кодом программы, электронное письмо.

Транзитные компьютеры могут соединяться между собой как сетью с коммутацией пакетов, так и сетью с коммутацией каналов. Сообщение хранится в транзитном компьютере на диске, причем время хранения может быть достаточно большим, если компьютер загружен другими работами или сеть временно перегружена.

По такой схеме обычно передаются сообщения, не требующие немедленного ответа. Обычно это сообщения электронной почты (в интернете или в сети FIDO). Режим коммутации сообщений разгружает сеть для передачи трафика, требующего быстрого ответа, например трафика службы WWW или файловой службы.

Техника коммутации сообщений появилась в компьютерных сетях раньше техники коммутации пакетов, но потом была вытеснена последней, как более эффективной по критерию пропускной способности сети.

[52] Буквально «вне сети» – когда абонент недоступен по локальной или глобальной вычислительной сети.

Сегодня коммутация сообщений работает только для некоторых не оперативных служб, причем чаще всего поверх сети с коммутацией пакетов, как служба прикладного уровня.

1.12. Коммутация пакетов

Коммутация пакетов – это техника коммутации абонентов, разработанная для эффективной передачи компьютерного трафика. Это потребовалось потому, что техника коммутации каналов не позволяет достичь высокой общей пропускной способности сети. Проблема заключается в пульсирующем характере трафика, который генерируют типичные сетевые приложения (рис. 10).

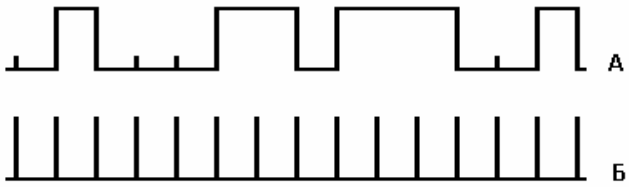


Рис. 10. Виды трафика: А – компьютерный (пульсирующий);
Б – мультимедийный (потоковый).

Коэффициент пульсации трафика отдельного пользователя сети, равный отношению средней интенсивности обмена данными к максимально возможной, может составлять 1:100 и более.

При коммутации пакетов все передаваемые пользователем сети 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. п. Сообщения могут иметь произвольную длину – от нескольких байт до нескольких гигабайт. Пакеты тоже могут иметь переменную длину, но в узких пределах, обычно от 46 до 1500 байт (но не более 4 кб). Каждый пакет снабжается заголовком, в котором указывается адресная информация, необходимая для доставки пакета узлу назначения, а также номер пакета, который будет использоваться узлом назначения для сборки сообщения (рис. 11). Пакеты транспортируются в сети как независимые информационные блоки. Коммутаторы принимают пакеты от конечных узлов и на основании адресной информации передают их друг другу, а в конечном итоге – узлу назначения.

Коммутаторы пакетной сети, в отличие от коммутаторов каналов, имеют внутреннюю буферную память для временного хранения пакетов. Если выходной порт коммутатора в момент принятия пакета занят, то пакет некоторое время находится в очереди пакетов в буферной памяти выходного порта, а когда до него доходит очередь, передается следующему коммутатору. Такая схема передачи данных позволяет сглаживать пульсации трафика на магистральных связях между коммутаторами и тем самым использовать их более эффективно.

Сеть с коммутацией пакетов замедляет процесс взаимодействия конкретной пары абонентов, так как их пакеты могут ожидать в коммутаторах, пока по магистральным связям передаются другие пакеты, пришедшие в коммутатор ранее. Однако общий объем данных, передаваемых сетью в единицу времени, будет выше, чем при технике коммутации каналов. Это происходит потому, что пульсации отдельных абонентов распределяются во времени, и коммутаторы постоянно и достаточно равномерно загружены работой.

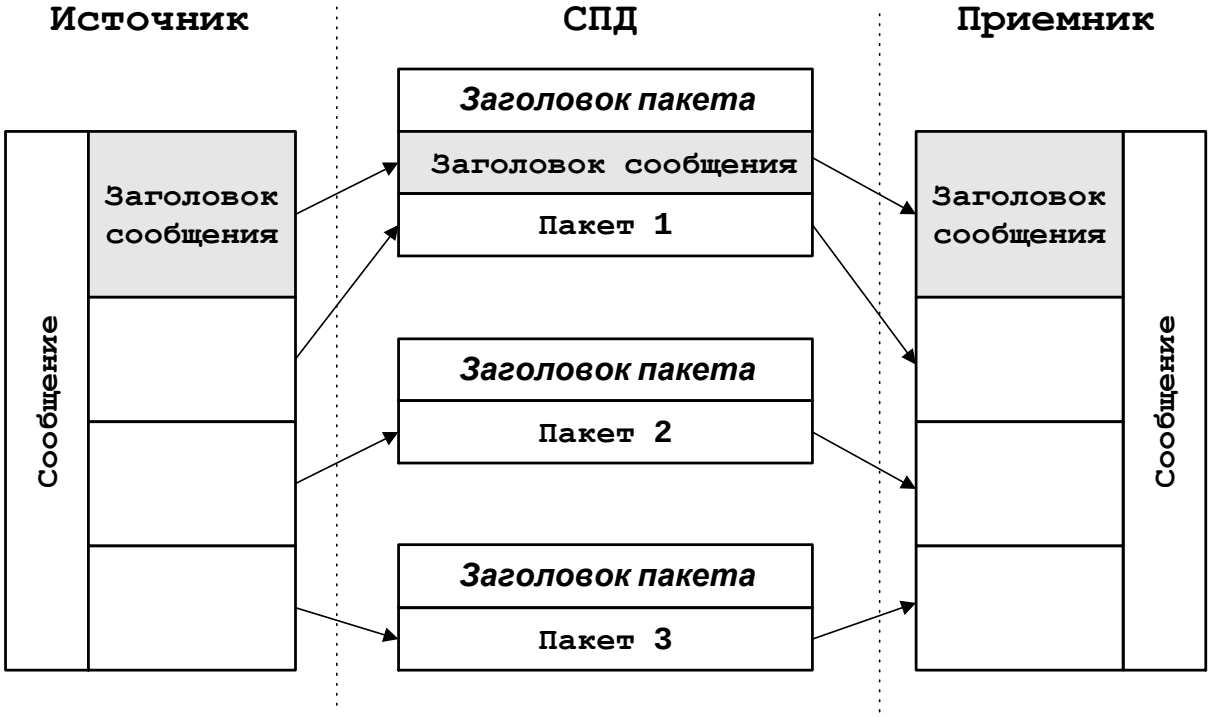


Рис. 11. Разбиение сообщения на пакеты

Методы коммутации пакетов

Используются два способа перемещения пакетов: дейтаграммный и виртуальный.

Дейтаграммный режим. Описанный выше режим передачи пакетов между двумя конечными узлами сети предполагает независимую маршрутизацию каждого пакета. Такой режим работы сети называется дейтаграммным. При его использовании коммутатор может изменить маршрут любого пакета в зависимости от состояния сети – работоспособности каналов и других коммутаторов, длины очередей пакетов в соседних коммутаторах и т. п.

В зависимости от маршрута и задержек в коммутаторах время перемещения по сети пакетов одного сообщения может быть различным, поэтому порядок прихода их к получателю в общем случае не соответствует порядку передачи.

Дейтаграммный метод не требует предварительного установления соединения, поэтому работает без задержки перед передачей данных. Это особенно выгодно для передачи небольшого объема данных, когда время установления соединения может быть соизмеримым со временем передачи данных. Кроме того, дейтаграммный метод быстро адаптируется к изменениям в сети.

Режим виртуального канала (virtual channel). Перед тем, как начать передачу данных между двумя конечными узлами, необходимо установить виртуальный канал, представляющий собой единственный маршрут, соединяющий эти узлы. Виртуальный канал может быть двух типов:

- *динамический виртуальный канал* устанавливается при передаче в сеть специального пакета – *запроса на установление соединения*. Этот пакет проходит через коммутаторы и «прокладывает» виртуальный канал. Коммутаторы запоминают маршрут для данного соединения и при поступлении следующих пакетов данного соединения отправляют их всегда по проложенному маршруту;
- *постоянный виртуальный канал* создается администратором сети путем ручной настройки коммутаторов.

При отказе коммутатора или канала на пути виртуального канала соединение разрывается, и виртуальный канал нужно прокладывать заново. При этом он обойдет отказавшие участки сети.

Пропускная способность сетей с коммутацией пакетов

Одним из отличий метода коммутации пакетов от метода коммутации каналов является неопределенность пропускной способности соединения между двумя абонентами. В методе коммутации каналов после образования

составного канала пропускная способность сети при передаче данных между конечными узлами известна – это пропускная способность канала. Данные после задержки, связанной с установлением канала, начинают передаваться на максимальной для канала скорости. Задержка распространения сигнала зависит от скорости распространения электромагнитных волн в конкретной физической среде

Передача данных в сети с коммутацией пакетов является более медленной, чем в сети с коммутацией каналов.

Количество управляющих сигналов при дейтаграммном режиме значительно меньше, чем при виртуальном, тем не менее, доля полезной информации в сетях передачи данных с коммутацией пакетов значительно меньше, чем в сетях с коммутацией каналов и сообщений.

Неопределенная пропускная способность сети с коммутацией пакетов – это плата за ее общую эффективность при некотором ущемлении интересов отдельных абонентов.

На эффективность работы сети существенно влияют размеры пакетов, которые передает сеть. Слишком большие размеры пакетов приближают сеть с коммутацией пакетов к сети с коммутацией каналов, поэтому эффективность сети падает. Слишком маленькие размеры заметно увеличивают долю служебной информации, так как каждый пакет несет с собой заголовок фиксированной длины, а количество пакетов, на которые разбиваются сообщения, резко растет при уменьшении размера пакета. Существует некоторая золотая середина, обеспечивающая максимальную эффективность работы сети, однако ее трудно определить точно, поскольку существует много факторов, влияющих на нее. Некоторые из них к тому же постоянно меняются в процессе работы сети. Поэтому разработчики протоколов для сетей с коммутацией пакетов выбирают пределы, в которых может находиться длина пакета. Нижний предел выбирается равным размеру служебного поля, что разрешает передавать служебные пакеты без пользовательских данных, а верхний предел не превышает 4-х килобайт. Приложения при передаче данных пытаются занять максимальный размер поля данных, чтобы быстрее выполнить обмен данными, а небольшие пакеты обычно используются для квитанций о доставке пакета.

При выборе размера пакета необходимо учитывать также и интенсивность битовых ошибок канала. На ненадежных каналах необходимо умень-

шать размеры пакетов, так как это уменьшает объем повторно передаваемых данных при искажениях пакетов. На качественных и надежных каналах для повышения производительности можно увеличить размер пакета до предела.

Глобальные сети с коммутацией пакетов

В конце 20-го века для надежного объединения локальных сетей и крупных компьютеров в корпоративную сеть использовалась практически одна технология глобальных сетей с коммутацией пакетов – X.25. Сегодня выбор стал гораздо шире, помимо сетей X.25 он включает такие технологии, как *frame relay* и ATM. Кроме этих технологий, разработанных специально для глобальных компьютерных сетей, доступны также услуги территориальных сетей TCP/IP. В табл. 3. приводятся характеристики этих сетей.

Таблица 3. Характеристики сетей с коммутацией пакетов

Сеть	**Скорость доступа**	**Тип Трафика**	**Примечания**
X.25	1,2-64 Кбит/с	Терминальный	Для каналов низкого качества; избыточность протоколов
Frame Relay	56 Кбит/с – 2 Мбит/с	Компьютерный	
SMDS	1,5-45 Мбит/с	Все типы	Распространены в США. Вытесняются сетями ATM.
ATM	155-622 Мбит/с; 2,4 Гбит/с	Все типы	Новейшие сети. Эксплуатация началась с 1996 г.
TCP/IP	1,2 Кбит/с – 2 Мбит/с	Терминальный, Компьютерный	Распространены в некоммерческом варианте – сеть Internet

Сети X.25

Сети X.25 являются на сегодняшний день самыми распространенными (особенно в Европе) сетями с коммутацией пакетов, используемыми для построения корпоративных сетей. Долгое время сети X.25 были единственными доступными сетями с коммутацией пакетов коммерческого типа, в которых давались гарантии коэффициента готовности сети. Кроме того, они хорошо работают на ненадежных линиях благодаря протоколам с установлением соединения и коррекцией ошибок на двух уровнях – канальном и сетевом.

Технология сетей X.25 имеет несколько существенных признаков, отличающих ее от других технологий:

- наличие в структуре сети специального устройства PAD[53], предна-

[53] PAD – Packet assembler-disassembler, сборщик-разборщик пакетов.

значенного для выполнения операции сборки нескольких низкоскоростных потоков байт от алфавитно-цифровых терминалов в пакеты, передаваемые по сети и направляемые компьютерам для обработки;

- наличие трехуровневого стека протоколов с использованием на канальном и сетевом уровнях протоколов с установлением соединения, управляющих потоками данных и исправляющих ошибки. Стандарт поддерживает режим коммутируемых виртуальных каналов и режим постоянного виртуального канала;
- ориентация на однородные стеки транспортных протоколов во всех узлах сети, поскольку сетевой уровень рассчитан на работу только с одним протоколом канального уровня и не может, подобно протоколу IP, объединять разнородные сети. Сеть X.25 состоит из коммутаторов, расположенных в различных географических точках и соединенных высокоскоростными выделенными каналами. Выделенные каналы могут быть как цифровыми, так и аналоговыми;
- пакеты в X.25 имеют длину до 128 байт. Обычная скорость 64 Кбит/с.

Асинхронные терминалы (не рассчитанные на X.25), подключаются к сети через устройства PAD. Терминалы не имеют конечных адресов сети X.25. Адрес присваивается порту PAD, который подключен к коммутатору пакетов X.25 с помощью выделенного канала.

Устройства PAD часто используются для подключения к сетям X.25 кассовых терминалов и банкоматов. Они могут использоваться для подключения датчиков телеметрии с помощью приборного интерфейса IEEE-488 (КОП) или аппаратуры телеуправления, имеющей асинхронный интерфейс RS-232.

В стеке протоколов сети X.25 стандарты описывают три уровня протоколов (рис. 12).

На *физическом* уровне определены синхронные интерфейсы X.21 и X.21bis к оборудованию передачи данных – либо к цифровому оборудованию, если канал является цифровым; либо к синхронному кабельному модему, если канал выделенный. Протокол физического уровня канала связи не оговорен, что дает возможность использовать каналы разных стандартов. На канальном уровне обычно используется протокол LAP-B.

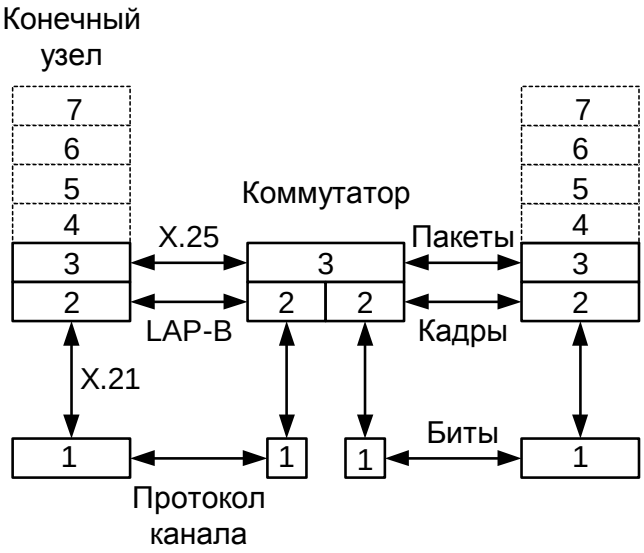


Рис. 12. Стек протоколов сети X.25.

На *канальном* уровне используется подмножество протокола HDLC, обеспечивающее возможность автоматической коррекции ошибок в линии. Предусмотрен выбор из двух процедур доступа к каналу: LAP или LAP-B.

На *сетевом* уровне (в стандарте он назван *пакетным*) определен протокол X.25/3 обмена пакетами между оконечным оборудованием и сетью передачи данных. Сетевой уровень отвечает за адресацию, управление потоком, подтверждение доставки, прерывания и т.п. Так как надежную передачу данных обеспечивает протокол LAP-B, протокол X.25/3 выполняет функции маршрутизации пакетов, установления и разрыва виртуального канала между конечными абонентами сети и управления потоком пакетов.

Транспортный уровень стандартом не определяется, но может быть реализован в конечных узлах.

Коммутаторы сетей X.25 представляют собой гораздо более простые и дешевые устройства по сравнению с маршрутизаторами сетей TCP/IP. Они не поддерживают обмен маршрутной информацией и поиск оптимальных маршрутов, не выполняют преобразований форматов кадров канальных протоколов. По принципу работы они ближе к коммутаторам локальных сетей, чем к маршрутизаторам. Однако работа, которую выполняют коммутаторы X.25 с кадрами, включает больше этапов, чем при продвижении кадров коммутаторами локальных сетей. Поэтому производительность коммутаторов X.25 оказывается обычно невысокой – несколько тысяч пакетов в секунду.

Протоколы сетей X.25 были специально разработаны для низкоскоростных линий с высоким уровнем помех. Именно такие линии составляют по-

ка большую часть телекоммуникационной структуры нашей страны, поэтому сети X.25 будут по-прежнему еще долго являться наиболее рациональным выбором для многих регионов.

Сети frame relay

Ретрансляция кадров (*frame relay*) – метод доставки сообщений в сетях передачи данных с коммутацией пакетов. Сети frame relay – сравнительно новые сети, они гораздо лучше, чем сети X.25, подходят для передачи пульсирующего трафика локальных сетей. Правда, это преимущество сказывается только на качественных волоконно-оптических каналах.

Преимущество сетей frame relay заключается в низкой протокольной избыточности и дейтаграммном режиме работы, что обеспечивает высокую пропускную способность и небольшие задержки кадров. Надежную передачу кадров технология frame relay не обеспечивает. Сети frame relay специально разрабатывались как общественные сети для соединения частных локальных сетей. Они обеспечивают скорость передачи данных до 2 Мбит/с.

Особенностью технологии frame relay является гарантированная поддержка основных показателей качества транспортного обслуживания локальных сетей – средней скорости передачи данных по виртуальному каналу при допустимых пульсациях трафика. Кроме технологии frame relay, гарантии качества обслуживания на сегодня может предоставить только ATM. Технология frame relay в сетях ISDN стандартизована как служба.

Для передачи данных в технологии frame relay используется техника виртуальных соединений, такая же, как в сетях X.25. Однако стек протоколов frame relay передает кадры при установленном виртуальном соединении по протоколам только физического и канального уровней, в то время как в сетях X.25 и после установления соединения пользовательские данные передаются протоколом 3-го уровня.

Frame relay – это протокол уровня звена данных (уровень 2 в модели OSI), предоставляющий простой, ориентированный на соединение сервис по передаче кадров. Данный протокол используется в основном для замены глобальных сетей с частными линиями. Такие функции, как управление потоком и устранение ошибок, возлагаются на высокоуровневые протоколы в устройствах конечных пользователей (табл. 4).

Таблица 4. Сопоставление стеков OSI и frame relay

<table>
<tr><th>Модель OSI</th><th colspan="2">Стек TCP/IP и frame relay</th></tr>
<tr><td>Прикладной</td><td colspan="2" rowspan="2">FTP, NFS</td></tr>
<tr><td>Презентационный</td></tr>
<tr><td>Сеансовый</td><td colspan="2">SMTP, Telnet, SNMP, TFTP</td></tr>
<tr><td rowspan="2">Транспортный</td><td>TCP</td><td>UDP</td></tr>
<tr><td rowspan="2">Сетевой</td><td colspan="2" rowspan="2">IP</td></tr>
<tr><td rowspan="2">Канальный</td></tr>
<tr><td colspan="2">PVC (обозначение маршрута)</td></tr>
<tr><td>Физический</td><td colspan="2">Frame relay</td></tr>
</table>

Кроме того, в сетях frame relay кадры передаются без преобразования и контроля, как и в коммутаторах локальных сетей. За счет этого сети frame relay обладают весьма высокой производительностью, так как кадры в коммутаторах не подвергаются преобразованию, а сеть не передает квитанции подтверждения между коммутаторами на каждый пользовательский кадр, как это происходит в сети X.25. Пульсации трафика передаются сетью frame relay достаточно быстро и без больших задержек. При таком подходе уменьшаются накладные расходы при передаче пакетов локальных сетей, так как они вкладываются сразу в кадры канального уровня, а не в пакеты сетевого уровня, как это происходит в сетях X.25.

Способность технологии frame relay гарантировать основные параметры качества обслуживания является ключевой. Именно поэтому технология получила широкое распространение и считается одной из самых перспективных в глобальных сетях.

Технология frame relay используется операторами связи для организации более дешевых по сравнению с каналами TDM систем абонентского доступа. Использование данной технологии позволяет значительно уменьшить затраты на организацию связи между несколькими территориально-разобщенными филиалами и более рационально использовать пропускную способность каналов передачи данных. Абонентские окончания сети frame

relay могут иметь скорости от 19,2 кБит/с до 2048 кБит/с с интерфейсами RS-232, V.35 и E1.

Применение сетей frame relay оправдано только при наличии на магистральных каналах волоконно-оптических кабелей высокого качества. Каналы доступа могут быть и на витой паре, как это разрешает интерфейс G.703 или абонентское окончание ISDN. Используемая на каналах доступа аппаратура передачи данных должна обеспечить приемлемый уровень искажения данных – вероятность ошибки не более 10^{-6}.

На величины задержек сеть frame relay гарантий не дает, и это основная причина, которая сдерживает применение этих сетей для передачи голоса. Передача видеоизображения тормозится также скоростью доступа в 2 Мбит/с, что для передачи видео часто недостаточно.

Сети ATM

Крупные вычислительные сети являются гетерогенными, и на согласование разнородных компонентов системные интеграторы затрачивают большие усилия.

Технология *асинхронного режима передачи*[54] первоначально была разработана как единый универсальный транспорт для нового поколения сетей с интеграцией услуг[55]. ATM – очень гибкая технология; позволяющая передавать по сети различные типы трафика – голос, видео и данные, обеспечивая при этом достаточную пропускную способность для каждого из них и гарантируя своевременную доставку восприимчивой к задержкам информации. ATM может использоваться как для построения высокоскоростных локальных сетей, так и магистралей, объединяющих традиционные локальные сети.

Единообразие, обеспечиваемое ATM, состоит в том, что одна транспортная технология может обеспечить следующие возможности:

- передача по одной сети компьютерного и мультимедийного трафика, чувствительного к задержкам, причем для каждого вида трафика качество обслуживания соответствует его потребностям;
- иерархия скоростей передачи данных, от десятков мегабит до нескольких гигабит в секунду с гарантированной пропускной способностью для ответственных приложений;

[54] ATM – Asynchronous transfer mode, асинхронный режим передачи.
[55] B-ISDN – Broadband ISDN, широкополосные сети ISDN.

- общие транспортные протоколы для локальных и глобальных сетей;
- сохранение имеющейся инфраструктуры физических каналов или физических протоколов и взаимодействие с унаследованными протоколами локальных и глобальных сетей: IP, Ethernet, ISDN.

Два основных режима передачи: коммутация каналов и коммутация пакетов имеют свои преимущества и недостатки. Коммутация каналов более всего подходят для передачи аудио и видеоинформации для которых существенными являются высокая постоянная скорость передачи и соблюдение последовательности передаваемых пакетов (*изохронность обмена*). Для постоянных каналов связи дополнительным преимуществом является постоянная готовность канала к обмену данными.

Недостатком коммутации каналов является неполное использование пропускной способности каналов между узлами в те промежутки времени, когда канал не занят или интенсивность обмена невелика.

Коммутация пакетов (особенно в дейтаграммном режиме) позволяет полностью использовать пропускную способность каналов сети. Этот режим более всего подходит для обмена данными, однако с его помощью очень трудно обеспечить передачу мультимедийной информации. Логические (виртуальные) каналы несколько улучшают положение, однако при перегрузке сети могут не обеспечить изохронность передачи.

Технология ATM совмещает в себе подходы двух технологий – коммутации пакетов и коммутации каналов. От первой она взяла передачу данных в виде адресуемых пакетов, а от второй – использование пакетов небольшого фиксированного размера, в результате чего задержки в сети становятся более предсказуемыми.

С помощью техники виртуальных каналов, предварительного заказа параметров качества обслуживания канала и приоритетного обслуживания виртуальных каналов с разным качеством обслуживания удается добиться передачи в одной сети разных типов трафика без ограничений. Технология ATM с самого начала разрабатывалась как технология, способная обслуживать все виды трафика в соответствии с их требованиями.

В качестве режима обмена данными, соединяющими в себе достоинства как режима коммутации каналов, так и режима коммутации пакетов был предложен режим быстрой коммутации (ретрансляции) ячеек.

Ячейки (cells) – небольшие пакеты фиксированной длины, которая составляет 53 байта, из них 5 байт – заголовок, 48 байт – данные. Фиксированная длина позволяет использовать относительно простые высокопроизводительные коммутирующие устройства. При использовании высокоскоростных каналов связи и соответствующих правил очередей в коммутирующих устройствах с помощью ячеек можно эмулировать (для передачи изохронного трафика) режим коммутации каналов.

В тоже время, коммутация ячеек обладает гибкостью пакетной коммутации, поскольку ячейки представляют собой пакеты с заголовками, позволяющими установление виртуальных каналов связи (с мультиплексированием). Кроме того, поскольку используются высокоскоростные каналы, скорость обмена определяется не скоростью канала, а той скоростью, с которой узел может передавать данные.

Таким образом, в основе технологии ATM лежат следующие базовые принципы:

- сети с трансляцией ячеек;
- сети с установлением соединения;
- коммутируемые сети.

Архитектура ATM предусматривает связь с существующими сетями с помощью межсетевых устройств, таких как коммутаторы, и разделения сетей на сети общего пользования и ведомственные сети.

Коммутаторы ячеек анализируют заголовок каждой прибывшей на входной порт ячейки, определяют маршрут ее следования и отправляют в соответствующий выходной порт. Принципиальным отличием коммутаторов ячеек от средств пакетной коммутации является очень высокая скорость коммутации, поэтому все функции коммутации реализуются в устройствах ATM аппаратно.

ATM Forum[56] разработал много интерфейсов, основанных на модели ATM, в том числе следующие:

- UNI – User-to-network interface, интерфейс «пользователь–сеть», определяет интерфейс между конечной станцией и коммутатором;
- PNNI – Private network-to-network interface, частный интерфейс «сеть–сеть», определяет интерфейс между коммутаторами;
- NNI – Network-to-network interface, интерфейс «сеть–сеть», опреде-

[56] Консорциум производителей оборудования ATM.

ляет интерфейс между сетями АТМ.

Эти стандарты определяют, как рабочие станции и коммутаторы взаимодействуют в сети АТМ.

Сеть может содержать только один уровень. Сеть АТМ, имеющая только один уровень, способна поддерживать до 200 коммутаторов.

На самом низком уровне сетевой топологии коммутаторы разделены на кластеры, называемые «группами равных». Коммутаторы, относящиеся к такой группе, обмениваются друг с другом маршрутизационной информацией. Коммутатор, являющийся граничным узлом (входит более чем в одну группу), обменивается маршрутизационной информацией со всеми группами равных, к которым он принадлежит. Таким образом группы узнают, как направлять ячейки адресатам, находящимся в пределах досягаемости одной из групп.

Эта схема повторяется до самого высокого уровня, на котором вся сеть представляется одной группой равных. Коммутаторы, находящиеся на самом низком уровне сетевой топологии, используют для определения маршрутов информацию с более высоких уровней. В результате коммутаторы не должны знать топологию всей сети.

АТМ имеет собственную сетевую модель. Стек протоколов АТМ показан в табл. 5, а распределение протоколов по конечным узлам и коммутаторам АТМ – на рис. 13.

Таблица 5. Структура стека протоколов АТМ

<table>
<tr><td colspan="3">ВЕРХНИЕ УРОВНИ СЕТИ</td></tr>
<tr><td rowspan="3">Уровни адаптации АТМ (AAL1–5)</td><td rowspan="2">CS – подуровень конвергенции (сходимости)</td><td>Общая часть подуровня конвергенции</td></tr>
<tr><td>Специфическая для сервиса часть</td></tr>
<tr><td colspan="2">Подуровень сегментации и реассемблирования (SAR)</td></tr>
<tr><td colspan="3">Уровень АТМ
(маршрутизация пакетов, мультиплексирование, управление потоком)</td></tr>
<tr><td rowspan="2">Физический уровень</td><td colspan="2">Подуровень согласования передачи</td></tr>
<tr><td colspan="2">Подуровень, зависящий от физической среды</td></tr>
</table>

Модель АТМ состоит из трех уровней:

- физический;
- уровень АТМ;
- уровень адаптации АТМ.

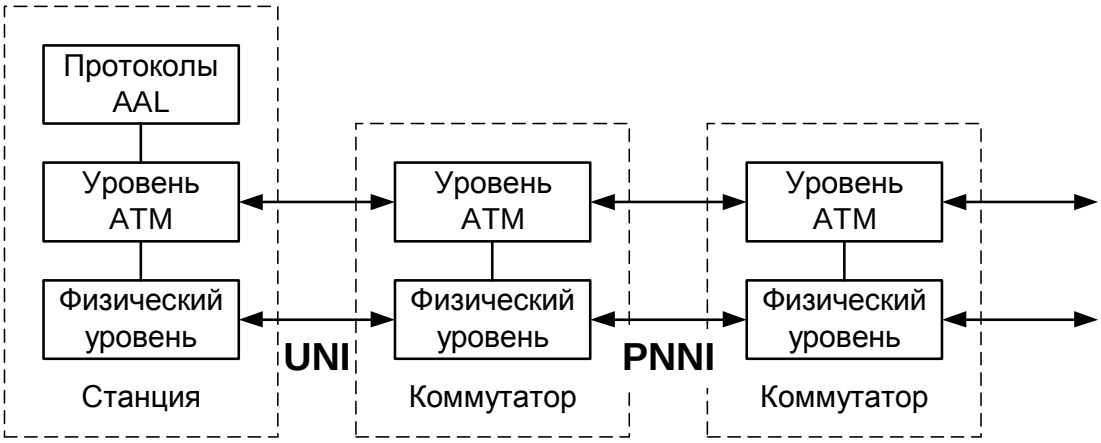


Рис. 13. Распределение протоколов по узлам и коммутаторам сети ATM.

Стек протоколов ATM примерно соответствует по функциям нижним уровням семиуровневой модели OSI (физическому, канальному и сетевому) и включает уровень адаптации ATM, собственно уровень ATM и физический уровень. Однако прямого соответствия между уровнями протоколов технологии ATM и уровнями модели OSI нет (табл. 6).

Таблица 6. Сравнение моделей OSI и ATM

<table>
<tr><th>Модель OSI</th><th colspan="2">Модель ATM</th></tr>
<tr><td>Прикладной уровень</td><td colspan="2" rowspan="3">Более высокие уровни</td></tr>
<tr><td>Уровень представления</td></tr>
<tr><td>Сеансовый уровень</td></tr>
<tr><td rowspan="2">Транспортный уровень</td><td colspan="2" rowspan="2">Уровень адаптации ATM</td></tr>
<tr><td rowspan="2">Сетевой уровень</td></tr>
<tr><td colspan="2" rowspan="2">ATM</td></tr>
<tr><td rowspan="2">Канальный уровень</td><td rowspan="2">Физический уровень</td></tr>
<tr><td>Физический уровень</td><td>Подуровень согласования</td></tr>
<tr><td>Физический уровень</td><td colspan="2">Подуровень физической среды</td></tr>
</table>

В настоящее время модель ATM не включает никаких дополнительных уровней, т.е. таких, которые соответствуют более высоким уровням модели OSI. Однако самый высокий уровень в модели ATM может связываться непосредственно с физическим, канальным, сетевым или транспортным уровнем модели OSI, а также непосредственно с ATM-совместимым приложением.

Физический уровень ATM управляет приемом и передачей битов по физической среде, а также отслеживает границы ячеек и упаковывает ячейки для формирования соответствующего типа кадра для используемой пере-

дающей среды. Этот уровень разделяется на два подуровня: подуровень физической среды и подуровень сходимости передачи.

Подуровень физической среды отвечает за передачу и прием непрерывного потока байтов, включающего информацию, синхронизирующую прием и передачу. Спецификации подуровня зависят от среды передачи и могут поддерживать любую физическую среду, способную передавать ячейки ATM.

Подуровень согласования передачи обеспечивает:

- поддержку границ ячеек ATM;
- генерацию заголовка управляющего кода ошибки для обеспечения достоверности данных;
- вставку или подавление пустых ячеек ATM для адаптации скорости обмена к пропускной способности передающей системы;
- упаковку ячеек ATM в кадры, принятые в данной передающей среде;
- генерацию и поддержку структуры кадров для данного физического уровня.

Стандарты ATM для физического уровня также описывают, какие кабельные системы должны использоваться в сетях ATM и с какими скоростями может работать ATM при каждом типе кабеля. 155-мегабитная ATM работает на кабелях UTP категории 5, экранированной витой паре (STP типа 1), оптоволоконном кабеле и беспроводных инфракрасных лазерных каналах. 622-мегабитная ATM работает только на оптоволоконном кабеле и может использоваться в локальных сетях.

Протокол ATM занимает в стеке протоколов ATM примерно то же место, что протокол IP в стеке TCP/IP. Протокол ATM занимается передачей ячеек через коммутаторы при установленном и настроенном виртуальном соединении, то есть на основании готовых таблиц коммутации портов. Протокол ATM выполняет коммутацию по номеру виртуального соединения.

Стандарты для уровня ATM регламентируют передачу сигналов, управление трафиком и установление соединений в сети ATM. Функции передачи сигналов и управления трафиком уровня ATM подобны функциям канального уровня модели OSI, а функции установления соединения ближе всего к функциям маршрутизации, которые определены стандартами модели OSI для сетевого уровня.

Стандарты установления соединения для уровня ATM определяют виртуальные каналы и виртуальные пути.

Виртуальный канал – это соединение между двумя конечными станциями ATM, которое устанавливается на время их взаимодействия. Виртуальный канал является двунаправленным; это означает, что после установления соединения каждая конечная станция может как посылать пакеты другой станции, так и получать их от нее.

Виртуальный путь – это путь между двумя коммутаторами, который существует постоянно, независимо от того, установлено ли соединение. Другими словами, виртуальный путь – это запомненный путь, по которому проходит весь трафик от одного коммутатора к другому.

Когда пользователь запрашивает виртуальный канал, коммутаторы определяют, какой виртуальный путь использовать для достижения конечных станций. По одному и тому же виртуальному пути в одно и то же время может передаваться трафик более чем для одного виртуального канала. Например, виртуальный путь с полосой пропускания 120 Мбит/с может быть разделен на четыре одновременных соединения по 30 Мбит/с каждый.

Уровень адаптации ATM выполняет следующие функции:

- определяет, как форматируются пакеты;
- предоставляет информацию для уровня ATM, которая дает возможность этому уровню устанавливать соединения с различным QoS;
- предотвращает заторы.

Уровень адаптации ATM состоит из четырех протоколов (называемых протоколами AAL[57]). Они принимают ячейки с уровня ATM, заново формируют из них данные, которые могут быть использованы протоколами, действующими на более высоких уровнях, и посылают их более высокому уровню. Когда протоколы AAL получают данные с более высокого уровня, они разбивают их на ячейки и передают уровню ATM.

В стандартах B-ISDN определены протоколы AAL 1, AAL 2, AAL 3/4 и AAL 5. Каждый протокол AAL упаковывает данные в ячейки своим способом. Все они, за исключением AAL 5, добавляют некоторую служебную информацию к 48 байтам данных в ячейке ATM. Эти издержки включают в себя специальные команды обработки для каждой ячейки, которые используются для обеспечения различных категорий сервиса.

Уровень адаптации ATM определяет четыре категории сервиса:

- постоянная скорость передачи битов (Constant bit rate – CBR). Ис-

[57] AAL – ATM adaptation level, уровень адаптации ATM.

пользуется для восприимчивого к задержкам трафика, при котором данные передаются с постоянной скоростью и требуют малого времени ожидания. CBR гарантирует самый высокий уровень качества сервиса, но использует полосу пропускания неэффективно;

- переменная скорость передачи битов (Variable bit rate – VBR). Существуют два вида VBR, использующиеся для различных типов трафика: VBR реального времени (Real-time VBR – RT-VBR) требует жесткой синхронизации между ячейками и поддерживает восприимчивый к задержкам трафик. VBR нереального времени (Non-real-time VBR – NRT-VBR) не нуждается в жесткой синхронизации между ячейками и поддерживает допускающий задержки трафик, такой как трансляция кадров (frame relay). Поскольку VBR не резервирует полосу пропускания, она используется более эффективно, чем в случае с CBR. Однако VBR не может гарантировать качество сервиса;
- неопределенная скорость передачи битов (Unspecified bit rate – UBR). UBR применяется для трафика, допускающего задержки. UBR не резервирует дополнительной полосы пропускания для виртуального канала, в результате один и тот же виртуальный канал может многократно применяться для нескольких передач. Однако, поскольку UBR не гарантирует качество сервиса, в сильно загруженных сетях UBR-трафик теряет большое число ячеек и имеет много повторных передач;
- доступная скорость передачи битов (Available bit rate – ABR). ABR также используется для передачи трафика, который допускает задержки, и дает возможность многократно использовать виртуальные каналы. Однако ABR обеспечивает для соединения допустимые значения ширины полосы пропускания и коэффициента потерь.

Эти категории используются для обеспечения различных уровней качества сервиса для разных типов трафика (в табл. 7 приведены характеристики каждой категории).

CBR, VBR, UBR, и ABR включают в себя различные параметры трафика, например среднюю и пиковую скорости, с которыми конечная станция может передавать данные. Эти категории сервиса также включают в себя следующие параметры качества сервиса:

- *коэффициент потерь ячеек* (Cell loss ratio) определяет, какой процент высокоприоритетных ячеек может быть потерян за время передачи;

Таблица 7. Уровни сервиса ATM

<table>
<tr><td colspan="4">Классы обслуживания</td></tr>
<tr><td>A</td><td>B</td><td>C</td><td>D</td></tr>
<tr><td rowspan="2">AAL1</td><td rowspan="2">AAL2</td><td>AAL3</td><td>AAL4</td></tr>
<tr><td colspan="2">AAL5</td></tr>
<tr><td>CBR</td><td>VBR
(RT, NRT)</td><td>ABR</td><td>UBR</td></tr>
<tr><td colspan="3">С установлением соединения</td><td>Без установления соединения</td></tr>
<tr><td colspan="2">Сохранение синхронизации</td><td colspan="2">Задержки допустимы</td></tr>
<tr><td>Постоянная скорость передачи</td><td colspan="3">Переменная скорость передачи</td></tr>
<tr><td>Звук/видео</td><td>Сжатые звук/видео</td><td>Передача данных Frame relay</td><td>TCP/IP и трафик локальной сети</td></tr>
</table>

- *задержка передачи ячейки* (Cell transfer delay) определяет количество времени (или среднее количество времени), требуемое для доставки ячейки адресату;
- *изменение задержки передачи ячейки* (Cell delay variation) – допустимые изменения в распределении группы ячеек между конечными станциями. Высокое значение задержки CDV приводит к прерыванию аудио- и видеосигналов.

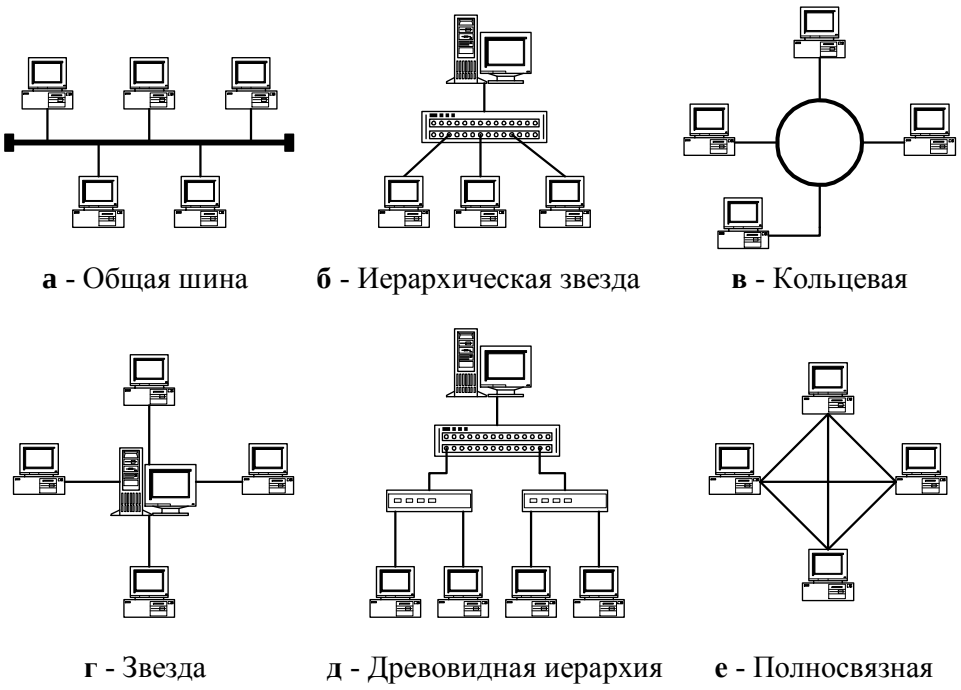
Перед установлением соединения конечная станция запрашивает одну из четырех категорий сервиса. Затем сеть ATM устанавливает соединение, используя соответствующие параметры трафика и качества сервиса. Сеть ATM использует параметры качества и для защиты трафика, т.е. предотвращения перегрузки сети. Сеть следит за тем, чтобы установленные соединения не превышали максимальной ширины полосы пропускания, которая им была предоставлена. Если соединение начинает ее превышать, сеть отказывается передавать ячейки. Кроме того, сеть ATM определяет, какие ячейки можно отбросить в случае ее переполнения: она проверяет параметры качества сервиса данного соединения и отбрасывает ячейки, для которых установлен высокий коэффициент потерь. И наконец, сеть отказывается устанавливать соединения, если не может их поддерживать.

Способность ATM обеспечивать для приложений различные уровни качества сервиса считается одним из достоинств технологии. Пользователи могут резервировать только ту полосу пропускания, которая им необходима; при этом сохраняется качество передаваемых аудио- и видеосигналов, а сеть предохраняется от переполнения. Однако, чтобы получить реальную выгоду

от качества сервиса в сети ATM, необходимы приложения, рассчитанные на его использование.

1.13. Топология сетей

Топология соединения хостов и маршрутизаторов – важный фактор конструкции сети. Основные топологии сетей показаны на рис. 14.



а - Общая шина **б** - Иерархическая звезда **в** - Кольцевая

г - Звезда **д** - Древовидная иерархия **е** - Полносвязная

Рис. 14. Основные сетевые топологии.

При объединении компьютеров в сеть необходимо выбрать способ организации физических связей, то есть *топологию*. Компьютеры, подключенные к сети, называют *станциями*, *узлами* или *хостами сети*.

Заметим, что конфигурация *физических связей* определяется электрическими соединениями компьютеров между собой и может отличаться от конфигурации *логических связей* между узлами сети. Логические связи представляют собой маршруты передачи данных между узлами сети и образуются путем соответствующей настройки коммуникационного оборудования.

Выбор топологии электрических связей существенно влияет на многие характеристики сети. Например, наличие резервных связей повышает надежность сети и делает возможным балансирование загрузки отдельных каналов, но в то же время требует наличие более сложной логики маршрутизации пакетов. Простота присоединения новых узлов делает сеть легко расширяемой. Экономические соображения часто приводят к выбору топологий, для кото-

рых характерна минимальная суммарная длина линий связи. Рассмотрим топологии немного подробней.

Полносвязная топология соответствует сети, в которой каждый компьютер сети связан со всеми остальными. Несмотря на логическую простоту, этот вариант оказывается громоздким и неэффективным. Действительно, каждый компьютер в сети должен иметь большое количество коммуникационных портов, достаточное для связи с каждым из остальных компьютеров сети. Для каждой пары компьютеров должна быть выделена отдельная электрическая линия связи. Полносвязные топологии применяются редко, чаще всего в многомашинных комплексах.

Ячеистая топология получается из полносвязной удалением некоторых возможных связей таким образом, что непосредственно связанными остаются только те компьютеры, между которыми происходит интенсивный обмен данными. Для обмена данными между компьютерами, не соединенными прямыми связями, используются транзитные передачи через промежуточные узлы. Ячеистая топология допускает соединение большого количества компьютеров и характерна, как правило, для глобальных сетей.

Общая шина подразумевает подключение компьютеров к одному коаксиальному кабелю по схеме. Передаваемая информация может распространяться в обе стороны. Такая схема снижает стоимость проводки, унифицирует подключение различных модулей, обеспечивает возможность почти мгновенного широковещательного обращения ко всем станциям сети. Основные преимущества – дешевизна и простота разводки кабеля по помещениям. Однако очень серьезный недостаток общей шины заключается в низкой ее надежности: любой дефект кабеля или одного из разъемов, сбой работы любого из хостов парализует всю сеть. Кроме того, общая шина характеризуется невысокой производительностью, так как в каждый момент времени только один компьютер может передавать данные в сеть. Поэтому пропускная способность канала связи всегда делится здесь между всеми узлами сети.

Топология звезда. В этом случае каждый компьютер подключается отдельным кабелем к общему устройству, называемому *концентратором*, находящемуся в центре сети. В функции концентратора входит направление передаваемой компьютером информации одному или всем остальным компьютерам сети. Главное преимущество звезды перед общей шиной – существенно большая надежность. Любые неприятности с кабелем касаются лишь

того компьютера, к которому этот кабель присоединен, и только неисправность концентратора может вывести из строя всю сеть. Кроме того, концентратор может играть роль интеллектуального фильтра информации, поступающей от узлов в сеть, и при необходимости блокировать запрещенные администратором передачи.

К недостаткам топологии относится более высокая стоимость сетевого оборудования из-за наличия дополнительного оборудования. Кроме того, возможности по наращиванию количества узлов в сети ограничиваются количеством портов концентратора. Иногда выгодно строить сеть с использованием нескольких концентраторов, иерархически соединенных между собой связями типа звезда. В настоящее время иерархическая звезда является самым распространенным типом топологии связей – как в локальных, так и в глобальных сетях.

В сетях с *кольцевой* конфигурацией данные передаются по кольцу от одного компьютера к другому в одном направлении. Если компьютер распознает данные как «свои», то он копирует их себе в буферную память. В сети с кольцевой топологией необходимо принимать специальные меры, чтобы в случае выхода из строя или отключения какой-либо станции не прервался канал связи между остальными станциями. Кольцо представляет собой очень удобную конфигурацию для организации обратной связи – данные, сделав полный оборот, возвращаются к узлу-источнику. Поэтому он может контролировать процесс доставки данных адресату. Часто это свойство кольца используется для тестирования связности сети и поиска узла, работающего некорректно. Для этого в сеть посылаются специальные тестовые сообщения.

Небольшие сети, как правило, имеют однородную типовую топологию – звезда, кольцо или общая шина. Для крупных вычислительных сетей характерно наличие произвольных связей между компьютерами. В них можно выделить отдельные произвольно связанные фрагменты (подсети), имеющие типовую топологию, поэтому их называют сетями со *смешанной топологией*.

1.14. Проблемы построения сетей

Совместное использование линий связи

В вычислительных сетях используют как индивидуальные линии связи между компьютерами, так и разделяемые. Несмотря на сложности, в локальных

сетях разделяемые линии связи используются очень часто. Этот подход, в частности, реализован в широко распространенных классических технологиях Ethernet и Token Ring. Следует отметить, что, по мере снижения стоимости оборудования и линий связи, идет процесс отказа от разделяемых сред передачи данных в локальных сетях. Это связано с тем, что за достигаемое разделением среды удешевление сети приходится расплачиваться производительностью.

Сеть с разделяемой средой при большом количестве узлов всегда будет работать медленнее, чем аналогичная сеть с индивидуальными линиями связи, так как пропускная способность индивидуальной линии связи достается одному компьютеру, а при совместном использовании – делится на все компьютеры сети.

При использовании индивидуальных линий связи в полносвязных топологиях конечные узлы должны иметь по одному порту на каждую линию связи. В звездообразных топологиях конечные узлы могут подключаться индивидуальными линиями связи к коммутатору. В глобальных сетях коммутаторы использовались уже на начальном этапе, а в локальных сетях – с начала 90-х годов. Коммутаторы приводят к удорожанию сети, но их стоимость неуклонно снижается, поэтому на сегодняшний день подавляющее большинство локальных сетей построено с использованием коммутаторов. В то же время, необходимо подчеркнуть, что индивидуальными в таких сетях являются только линии связи между конечными узлами и коммутаторами сети, а связи между коммутаторами остаются разделяемыми, так как по ним передаются сообщения разных конечных узлов.

В глобальных сетях отказ от разделяемых линий связи объясняется техническими причинами. Большие временные задержки распространения сигналов принципиально ограничивают применимость техники разделения линии связи. Компьютеры могут затратить больше времени на переговоры о том, кому сейчас можно использовать линию связи, чем непосредственно на передачу данных по ней. Однако это не относится к линиям связи типа «коммутатор–коммутатор». Тогда только два коммутатора борются за доступ к линии связи, что существенно упрощает задачу организации совместного использования линии.

Адресация компьютеров

Еще одной проблемой, которую нужно учитывать при объединении в

сеть трех и более компьютеров, является проблема их адресации. К адресу узла сети и схеме его назначения предъявляются следующие требования:

- адрес должен уникально идентифицировать компьютер в сети любого масштаба;
- схема назначения адресов должна сводить к минимуму ручной труд администратора и вероятность дублирования адресов;
- адрес должен иметь иерархическую структуру, удобную для построения больших сетей;
- адрес должен быть удобен для пользователей сети, а это значит, что он должен иметь символьное представление;
- адрес должен иметь по возможности компактное представление, чтобы не перегружать память коммуникационной аппаратуры.

Очевидно, что эти требования противоречивы – например, адрес, имеющий иерархическую структуру, скорее всего, будет менее компактным, чем *плоский адрес* (то есть, не имеющий структуры, неиерархический). Символьный же адрес, скорее всего, потребует больше памяти, чем адрес-число.

Так как все перечисленные требования трудно совместить в рамках какой-либо одной схемы адресации, то на практике используется сразу несколько схем, так что компьютер одновременно имеет несколько адресов-имен. Каждый адрес используется в той ситуации в которой он наиболее удобен. А чтобы не возникало путаницы используются специальные протоколы, позволяющие по адресу одного типа определить адреса других типов.

Наибольшее распространение получили следующие три схемы адресации узлов:

- *аппаратные (hardware) адреса*. Они предназначены для сети небольшого или среднего размера, поэтому не имеют иерархической структуры. Типичным представителем адреса такого типа является адрес сетевого адаптера локальной сети (MAC-адрес[58]). Такой адрес обычно используется только аппаратурой, поэтому его стараются сделать по возможности компактным и записывают в виде двоичного или шестнадцатеричного значения, например **`0087f05d24b5`**[59]. Помимо отсутствии иерархии, использование ап-

[58] MAC – Media access control, управление доступом к носителю. MAC-адрес – уникальный идентификатор, сопоставляемый с различными типами оборудования для компьютерных сетей. В широковещательных сетях MAC-адрес позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу.

[59] Стандарты IEEE определяют 48-разрядный MAC-адрес, который разделен на че-

паратных адресов связано еще с одним недостатком – при замене аппаратуры, например, сетевого адаптера, изменяется и адрес компьютера, что может привести к проблемам с идентификацией и аутентификацией пользователя. Более того, при установке нескольких сетевых адаптеров у компьютера появляется несколько адресов, что не очень удобно для пользователей сети;

- *символьные адреса* или *имена*. Эти адреса предназначены для запоминания людьми, поэтому обычно несут смысловую нагрузку. Символьные адреса легко использовать как в небольших, так и крупных сетях. Пример символьного имени – **kgeu.ru**;

- *числовые составные адреса*. Символьные имена удобны для людей, но из-за переменного формата и большой длины их передача по сети не очень экономична. Поэтому во многих случаях для работы в больших сетях в качестве адресов узлов используют числовые составные адреса фиксированного и компактного форматов. Типичным представителями адресов этого типа являются IP- и IPX-адреса. В них поддерживается двухуровневая иерархия, адрес делится на старшую часть – номер сети и младшую – номер узла. Это позволяет передавать сообщения между сетями только на основании номера сети, а номер узла используется уже в пределах нужной сети.

В современных сетях для адресации узлов применяются, как правило, одновременно все три приведенные выше схемы. Пользователи адресуют компьютеры символьными именами, которые автоматически заменяются в сообщениях, передаваемых по сети, на числовые номера. С помощью числовых номеров сообщения передаются из одной сети в другую, а после доставки сообщения в сеть назначения вместо числового номера используется аппаратный адрес компьютера.

Подробнее об IP-адресации см. 1.16.

Структуризация больших сетей

В сетях с небольшим (10–30) количеством компьютеров чаще всего используется одна из типовых топологий – общая шина, кольцо, звезда. Все пе-

---

тыре части. Первый бит указывает, для одиночного (0) или группового (1) адресата предназначен кадр. Второй бит показывает, является ли он универсальным (0) или локально управляемым (1). Третье поле указывает часть адреса, которую производитель оборудования получает при регистрации в IEEE. Три последних октета (октет – 8 бит) выбираются изготовителем устройства. Адрес устройства глобально уникален и обычно зашивается в аппаратуру.

речисленные топологии *однородны*, то есть все компьютеры в такой сети имеют одинаковые права в отношении доступа к другим компьютерам (за исключением центрального компьютера при соединении звезда). Однородность структуры делает простой процедуру наращивания числа компьютеров, облегчает обслуживание и эксплуатацию сети.

Однако при построении больших сетей однородная структура превращается из преимущества в недостаток. Использование типовых структур порождает различные ограничения, важнейшими из которых являются:

- ограничения на длину связи между узлами;
- ограничения на количество узлов в сети;
- ограничения на интенсивность трафика, порождаемого узлами сети.

Например, технология Ethernet на тонком коаксиальном кабеле позволяет использовать кабель длиной не более 185 метров, к которому можно подключить не более 30 компьютеров. Однако, если компьютеры интенсивно обмениваются информацией между собой, число подключенных к кабелю компьютеров приходится снижать до 20, а то и до 10, чтобы каждому компьютеру доставалась приемлемая доля общей пропускной способности сети.

Для снятия этих ограничений используются специальные методы структуризации сети и коммуникационное оборудование.

Простейшее из коммуникационных устройств – *повторитель (repeater)* – используется для физического соединения различных сегментов кабеля локальной сети с целью увеличения общей длины сети. Он передает сигналы, приходящие из одного сегмента сети, в другие сегменты, тем самым позволяя преодолеть ограничения на длину линий связи в 185 м за счет улучшения качества передаваемого сигнала – восстановления его мощности и амплитуды, улучшения фронтов и т. п.

Концентратор всегда изменяет физическую топологию сети, но не затрагивает логическую. Под *физической топологией* понимается конфигурация связей, образованных отдельными частями кабеля, а под *логической* – конфигурация информационных потоков между компьютерами сети. Во многих случаях физическая и логическая топологии сети совпадают.

Наиболее важной проблемой, не решаемой путем физической структуризации, остается проблема перераспределения передаваемого трафика между различными физическими сегментами сети. Логическая структуризация сети позволяет разбить сети на сегменты таким образом, что основ-

ная часть трафика компьютеров каждого сегмента не выходит за пределы этого сегмента.

В большой сети естественным образом возникает неоднородность информационных потоков: сеть состоит из множества подсетей рабочих групп, отделов, филиалов предприятия и других административных образований. Очень часто наиболее интенсивный обмен данными наблюдается между компьютерами, принадлежащими к одной подсети, и только небольшая часть обращений происходит к ресурсам компьютеров, находящихся вне локальных рабочих групп. Довольно долго такое соотношение трафиков не подвергалось сомнению, даже был сформулирован эмпирический закон «80/20», в соответствии с которым в каждой подсети 80% трафика является внутренним и только 20% – внешним[60]. Сейчас характер нагрузки сетей во многом изменился, на многих предприятиях имеются централизованные хранилища корпоративных данных, активно используемые сотрудниками. Это не могло не повлиять на распределение информационных потоков. Сегодня обычна ситуация, когда интенсивность внешних обращений выше интенсивности обмена между машинами в одном сегменте. Но независимо от того, в какой пропорции распределяются внешний и внутренний трафик, для повышения эффективности работы сети неоднородность информационных потоков учитывать необходимо.

Сеть с типовой топологией (шина, кольцо, звезда), в которой все физические сегменты рассматриваются в качестве одной разделяемой среды, оказывается неадекватна структуре информационных потоков в большой сети. Например, в сети с общей шиной взаимодействие любой пары компьютеров занимает ее на все время обмена, поэтому при увеличении числа компьютеров в сети шина становится узким местом. Компьютеры одного отдела вынуждены ждать, когда окончит обмен пара компьютеров другого отдела, а необходимость в связи между компьютерами двух разных отделов возникает гораздо реже и требует совсем небольшой пропускной способности.

Рассмотрим пример сети (рис. 15), построенной на концентраторах (*хабах*). При передаче кадра от хоста А к хосту В концентраторы распространяют этот кадр во все сегменты. Сеть блокируется до тех пор, пока хост В не примет данные.

[60] Соотношение 80/20 иногда называют «принципом Парето».

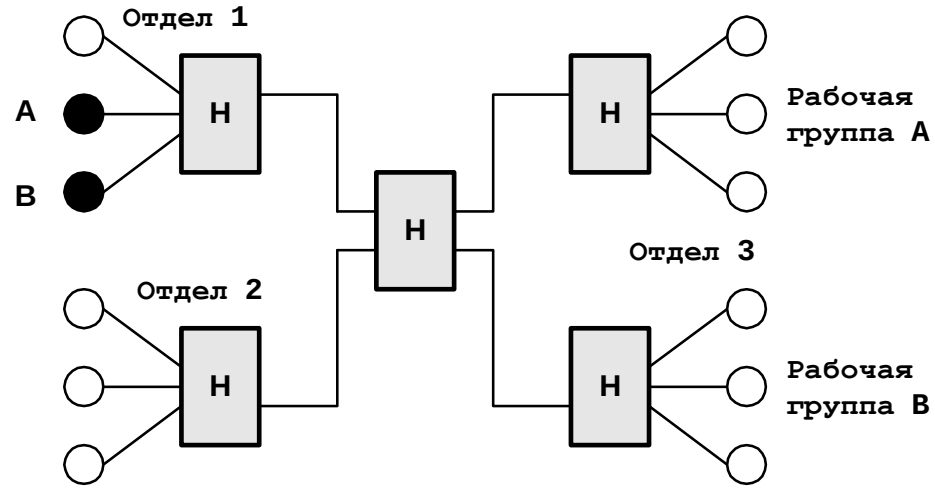


Рис. 15. Физическая структуризация сети с помощью концентраторов

Решение проблемы состоит в отказе от идеи единой однородной разделяемой среды. Например, можно не использовать общую разделяемую среду в пределах всей сети, но применять ее в пределах каждого отдела. Пропускная способность линий связи между отделами не должна совпадать с пропускной способностью среды внутри отделов. Если трафик между отделами составляет только 20% трафика внутри отдела, то и пропускная способность линий связи и коммуникационного оборудования, соединяющего отделы, может быть значительно ниже внутреннего трафика сети отдела.

Распространение трафика, предназначенного для компьютеров некоторого сегмента сети, только в пределах этого сегмента, называется *локализацией* трафика. *Логическая структуризация сети* – процесс разбиения сети на сегменты с локализованным трафиком.

Средствами логической структуризации служат мосты, коммутаторы, маршрутизаторы и шлюзы.

Мост (*bridge*) делит разделяемую среду передачи сети на логические сегменты (подсети), передавая информацию из одного сегмента в другой только в том случае, если адрес компьютера назначения принадлежит другому сегменту. Тем самым мост изолирует трафик одной подсети от трафика другой, тем самым повышая общую производительность передачи данных в сети (рис. 16). Локализация трафика не только экономит пропускную способность, но и уменьшает возможность несанкционированного доступа к данным, так как кадры не выходят за пределы своего сегмента, и их сложнее перехватить злоумышленнику.

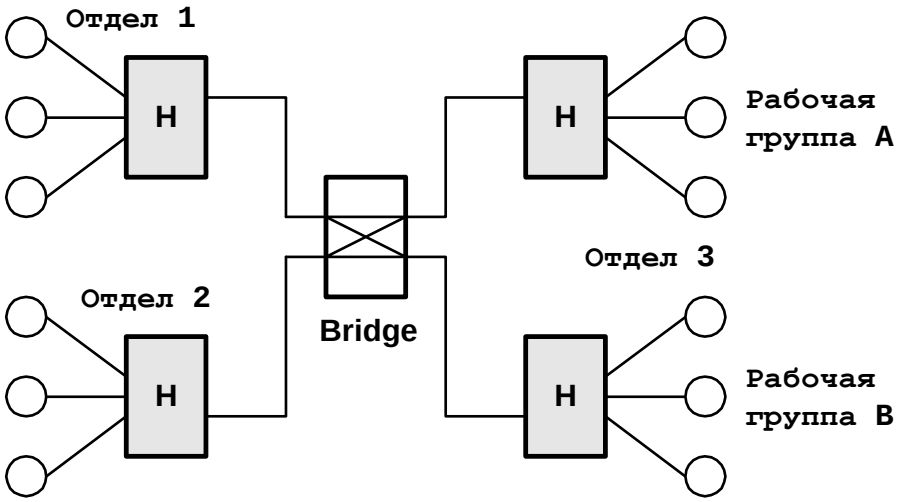


Рис. 16. Логическая структуризация сети с помощью моста

Мосты используют для локализации трафика аппаратные адреса компьютеров. Это затрудняет распознавание принадлежности того или иного компьютера к определенному логическому сегменту – сам адрес не содержит никакой информации по этому поводу. Мост достаточно упрощенно представляет деление сети на сегменты – он запоминает, через какой порт на него поступил кадр данных от каждого компьютера сети, и в дальнейшем передает кадры, предназначенные для этого компьютера, на соответствующий порт. Точной топологии связей между логическими сегментами мост не знает. Поэтому применение мостов приводит к значительным ограничениям на конфигурацию связей сети – сегменты должны быть соединены таким образом, чтобы в сети не образовывались замкнутые контуры.

Коммутатор (switch, switching hub) по принципу обработки кадров не отличается от моста. Основное отличие состоит в том, что он является коммуникационным мультипроцессором. Каждый порт оснащен специализированным процессором, обрабатывающим кадры по алгоритму моста независимо от процессоров других портов. За счет этого общая производительность коммутатора намного выше производительности традиционного моста, имеющего один процессорный блок.

Ограничения по топологии связей, связанные с применением мостов и коммутаторов, привели к тому, что в ряду коммуникационных устройств появился еще один тип оборудования – *маршрутизатор (router)*. Маршрутизаторы более надежно и более эффективно, чем мосты, изолируют трафик отдельных частей сети друг от друга. Маршрутизаторы используют не плоские аппаратные, а составные числовые адреса, и поэтому образуют логиче-

ские сегменты посредством явной адресации. В этих адресах имеется поле номера сети, так что все компьютеры, у которых значение этого поля одинаково, принадлежат к одной подсети.

Маршрутизаторы могут работать в сети с замкнутыми контурами, при этом осуществляют выбор оптимального маршрута из нескольких возможных (рис. 17).

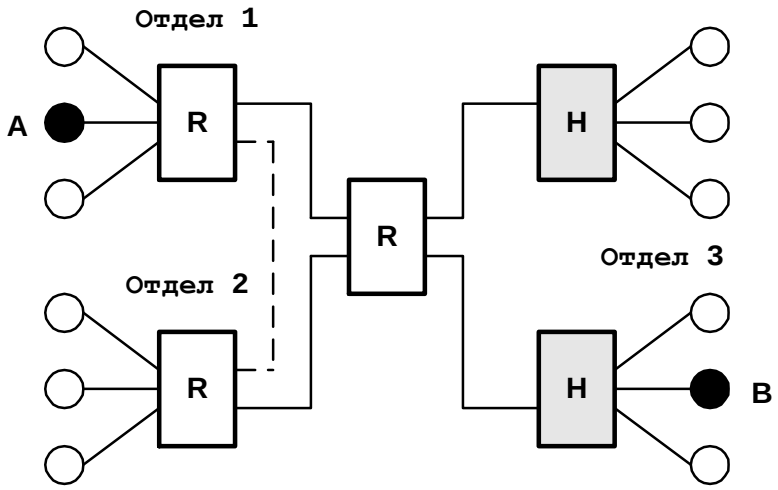


Рис. 17. Логическая структуризация сети с помощью маршрутизаторов.

Другой важной функцией маршрутизаторов является их способность связывать в единую сеть подсети, построенные с использованием разных сетевых технологий, например Ethernet и X.25.

Кроме перечисленных устройств отдельные части сети может соединять *шлюз (gateway)*. Основной причиной, по которой в сети используют шлюз, является необходимость объединить разные по архитектуре сети (т.е. сети с разными типами системного и прикладного программного обеспечения), а не желание локализовать трафик. Тем не менее, шлюз также обеспечивает локализацию трафика в качестве побочного эффекта.

Крупные сети никогда не строятся без логической структуризации. Для отдельных сегментов и подсетей характерны типовые однородные топологии базовых технологий, а для их объединения всегда используется оборудование, обеспечивающее локализацию трафика, – мосты, коммутаторы, маршрутизаторы и шлюзы.

1.15. Технологии беспроводного широкополосного доступа

Строить по доступным ценам сети с абонентскими каналами доступа не менее 2 Мбит/с позволяют несколько технологий. Это решения на основе систем кабельного телевидения, беспроводные сети семейства стандартов IEEE 802.11 (Wi-Fi) и 802.16, упомянутые в разделе 1.7, и ряд стандартов для организации цифровых линий, объединенных аббревиатурой xDSL[61]. Широкополосная беспроводная связь уже давно рассматривается в качестве реальной альтернативы традиционным способам высокоскоростного абонентского доступа, в том числе и проводным технологиям, таким как xDSL и оптоволоконным технологиям, например FTTP.

Местные и многоканальные многоточечные распределительные системы LMDS[62] и MMDS[63] (которые называют также «сотовым телевидением»), первоначально предназначавшиеся для трансляции телепрограмм в районах, не имеющих кабельной инфраструктуры, в последнее время иногда используются для организации широкополосной беспроводной передачи данных на «последней миле»[64]. Радиус действия передатчиков MMDS, работающих в диапазоне 2,1-2,7 ГГц, может достигать 40-50 км, в то время как максимальная дальность передачи сигнала в системах LMDS, использующих значительно более высокие частоты в области 27-31 ГГц, составляет 2,5-3 км.

Классификация беспроводных технологий приведена на рис. 18.

---

[61] ADSL – Asymmetric digital subscriber line, асимметричная цифровая абонентская линия. Используется для несимметричного доступа, позволяющего потребителю принимать сигналы со скоростью до 8 Мбит/с, а передавать – со скоростью до 1 Мбит/с на расстояние до 7 км. SDSL – Synchronous digital subscriber line, синхронная цифровая абонентская линия. HDSL – High-bit-rate digital subscriber line, технология высокоскоростной передачи по кабелям на основе скрученных медных пар, обеспечивающая передачу двунаправленных потоков информации на расстояние до 6 км со скоростью 2 Мбит/с.

[62] LMDS – Local multipoint distribution service, местная (локальная) многоточечная распределенная служба связи. Беспроводная система связи, функционирующая в диапазоне сверхвысоких частот 26-30 ГГц. При построении инфраструктуры LMDS используются соты размером 5-15 км, причем передающая и принимающая антенны должны находиться в зоне прямой видимости.

[63] MMDS – Multichannel multipoint distribution service, многоканальная многоточечная распределенная служба связи. Беспроводная система связи, функционирующая в диапазоне частот 2,5-2,7 ГГц.

[64] В Казани с 2000 года *Радиотелесет* эксплуатирует оборудование MMDS на базе канальных передатчиков EMCEE TTS 28HS, однако услуга передачи данных пока не предоставляется.

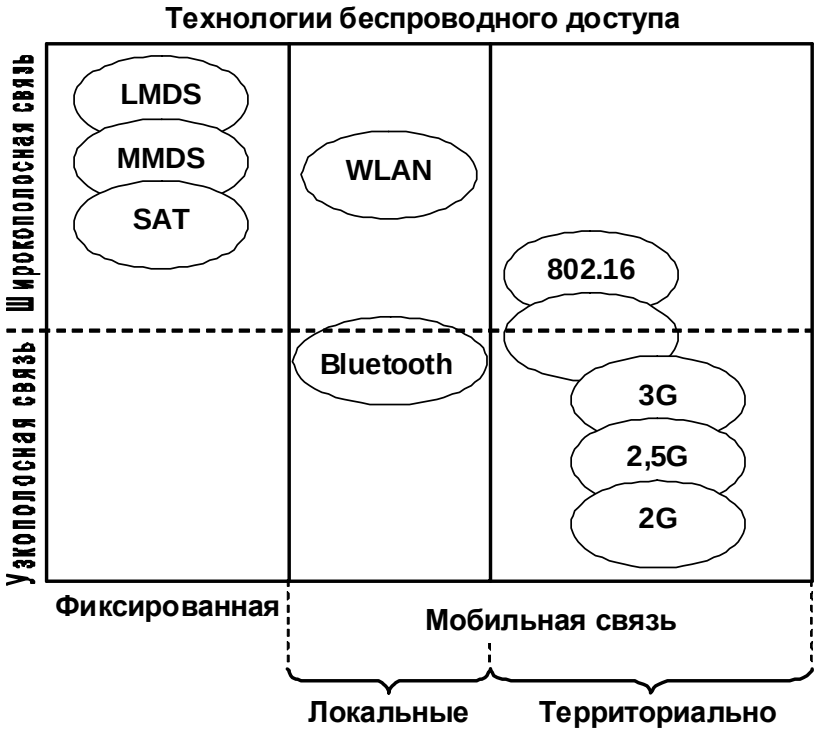


Рис. 18. Технологии беспроводного доступа.

Традиционные технологии передачи данных в беспроводных сетях (WLAN[65]) относятся к узкополосным, т.е. работают в полосе частот, много меньшей несущей. Расширение спектра передаваемого сигнала позволяет увеличить скорость передачи данных и повысить помехоустойчивость системы. Достигнутый на сегодняшний день показатель максимальной пропускной способности стандарта IEEE 802.11a, использующего на физическом уровне технологию расширения спектра методом прямой последовательности (DSSS), составляет 56 Мбит/с. Увеличение этого показателя требует расширения полосы частот, используемых системой, что нереально из-за «тесноты» радиочастотного спектра. Дальнейшее развитие WLAN связано с применением технологий на базе сверхширокополосных сигналов (UWB – Ultra wideband).

Рассмотрим основные показатели (дальность связи и скорость передачи данных) систем, работающих в диапазонах 2,4 ГГц и 5 ГГц, что позволит выявить сильные и слабые стороны в сравнении с кабельными технологиями Ethernet.

Американский стандарт IEEE 802.11b ориентирован на использование частотного диапазона 2,4 ГГц. Спектр сигнала уширяется путем до-

[65] WLAN – Wireless LAN, технологии беспроводных локальных сетей.

бавления к полезному сигналу шумоподобного кода. При этом происходит уменьшение спектральной плотности энергии излучаемого сигнала. Дальность действия составляет 50…300 м и обратно пропорциональна скорости передачи. Оборудование 802.11b может работать со скоростями 11; 5,5; 2 и 1 Мбит/с.

Стандарт 802.11a рассчитан на диапазон 5 ГГц. Он предусматривает обязательные скорости 6, 12 и 24 Мбит/с и необязательные – 9, 18, 36, 48 и 54 Мбит/с. Дальность действия составляет 30...160 м и сильнее зависит от погоды и рельефа местности. Аналогичные показатели и у европейского стандарта HiperLAN2.

На рис. 19 показаны результаты замеров пропускной способности реальных систем. Для сравнения приведены показатели для проводного Ethernet, а также для стандарта для подключения периферийных устройств Bluetooth.

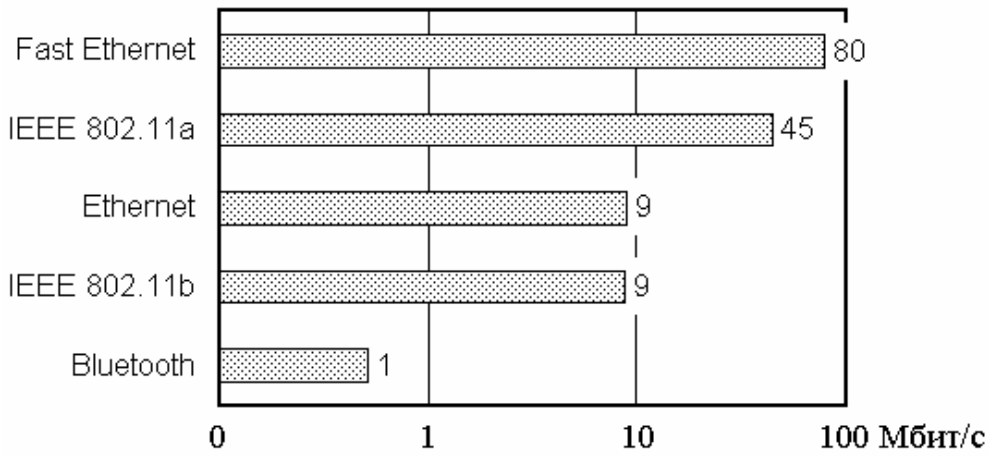


Рис. 19. Сравнение реально достижимых скоростей передачи данных в различных технологиях WLAN и проводного Ethernet.

Основными параметрами при сравнении беспроводных технологий являются: частотный диапазон, максимальная скорость передачи, покрытие при заданной скорости передачи. В беспроводных сетях принято измерять трафик в битах в секунду на единицу площади. Этот показатель для технологии UMB может достигать десятка Мбит/с/м^2, что на порядок превышает таковой для технологии IEEE 802.11a.

В таблице 8 перечислены основные параметры стандартов WLAN с пропускной способностью ~30 Мбит/с и ~2 Мбит/с.

Таблица 8. Основные параметры стандартов WLAN

Протокол	Частотный диапазон, ГГц	Зона покрытия, м	Макс. скорость, Мбит/с
IEEE 802.11g/e	2,4	20	54
IEEE 802.11a	5	20	54
HiperLAN2	5	20	54
IEEE 802.15.3	2,4	10	10
IEEE 802.16.3	2–11	>20	2
IEEE 802.11b	2,4	60	11

Применение технологии UWB, использующей сверхкороткие импульсы (длительность < 1 нс) специальной формы, позволяет распределить всю энергию сигнала по широкому участку спектра в диапазоне от 3,1 до 10,6 ГГц. При этом спектральная плотность энергии не превышает определенного частью 15 правил Федеральной комиссии связи предела (-41дБ Вт/МГц).

На рис. 20 показано распределение частотных диапазонов, используемых различными системами, включая навигационную GPS[66].

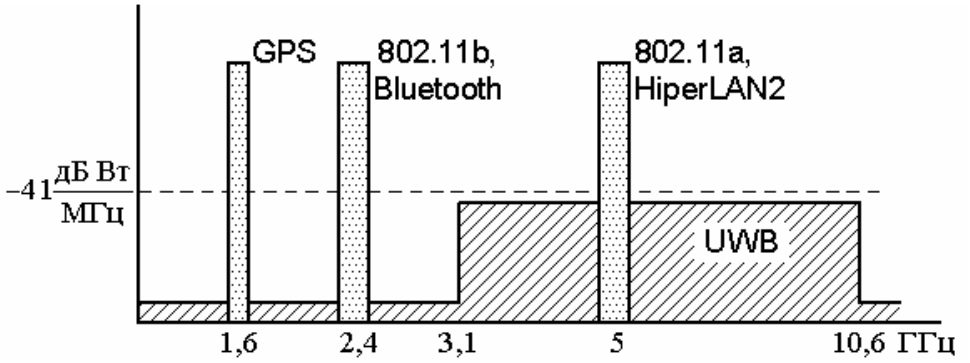


Рис. 20. Полоса спектра, используемая в технологии UWB.

Зависимость пропускной способности от дальности в технологии UWB принципиально отличается от таковой в стандартах IEEE 802.11 (рис. 21).

Учитывая вышесказанное, можно сделать вывод, что основным направлением развития WLAN является увеличение пропускной способности систем на основе перехода от узкополосных к широкополосным и сверхширокополосным сигналам, а также внедрение более совершенных схем модуляции и кодирования сигналов.

[66] GPS – Global Positioning System, глобальная система навигации и определения положения. Созданная министерством обороны США спутниковая система определения местонахождения объектов. Позволяет определить в любой точке земного шара местонахождение неподвижного либо движущегося объекта на земле, в воздухе и на море в трех измерениях с очень высокой точностью. Аналогичную систему в России GLONASS планируется ввести в эксплуатацию до 2010 года.

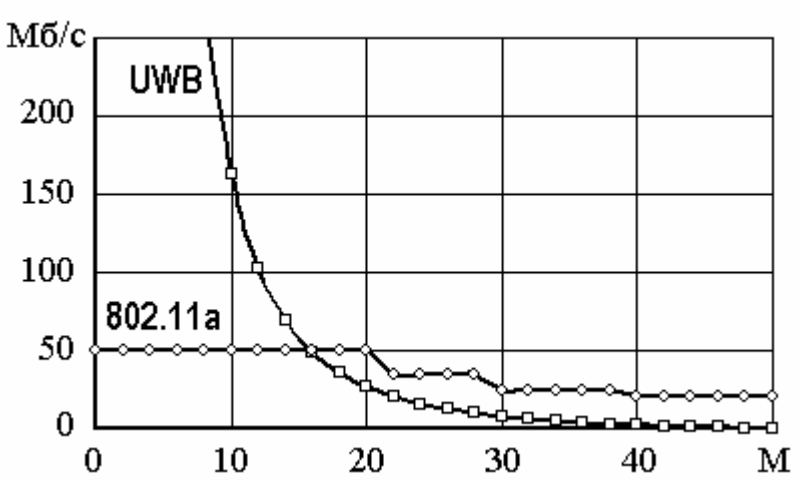


Рис. 21. Зависимость пропускной способности
от дальности для технологий UWB и IEEE 802.11a.

1.16. Адресация в IP-сетях

Каждый компьютер в сети TCP/IP имеет адреса следующих трех уровней:

- *локальный адрес узла*, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Обычно в качестве такого адреса выступает MAC-идентификатор (Ethernet-адрес) сетевого адаптера или порта маршрутизатора. Эти адреса назначаются производителями оборудования и являются уникальными. 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;
- *символьный идентификатор-имя*. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Такой адрес используется на прикладном уровне, например, в протоколах FTP или TELNET;
- для узлов, входящих в глобальные сети, такие как X.25 или frame relay, локальный адрес назначается администратором глобальной сети 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 Информационного сетевого центра[67], если сеть должна работать как составная часть интернета.

[67] NIC – Network information center.

Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла – гибкое, и граница между этими полями может устанавливаться весьма произвольно. Узел может входить в несколько IP-сетей. В этом случае он должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значение каждого байта в десятичной форме, и разделенных точками, например:

- **`128.10.2.30`** – десятичная форма представления адреса;
- **`10000000 00001010 00000010 00011110`** – двоичная форма представления этого же адреса.

Класс A: 0 N сети N узла

Класс B: 10 N сети N узла

Класс C: 110 N сети N узла

Класс D: 1110 N сети N узла

Класс E: 11110 N сети N узла

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 A имеют номера в диапазоне 1…126 (номер 0 не используется, а номер 127 зарезервирован для специальных целей, о чем будет сказано ниже). Максимальное количество компьютеров в одной сети 16777214;
- если первые два бита адреса равны 10, то сеть относится к классу B и является сетью средних размеров с числом узлов 28…216. В сетях класса B под адрес сети и под адрес узла отводится по 16 битов, то есть по 2 байта. Возможное количество сетей 166382, максимальное количество компьютеров в одной сети 65534;
- если адрес начинается с последовательности 110, то это сеть класса C с числом узлов не больше 28. Под адрес сети отводится 24 бита, а под адрес узла – 8 битов. Возможное количество сетей 2097150, максимальное количество компьютеров в одной сети 254;
- если адрес начинается с последовательности 1110, то он является адресом класса D и обозначается как 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 E, он зарезервирован для будущих применений.

В таблице 9 приведены диапазоны номеров сетей.

Таблица 9. Диапазоны номеров сетей в TCP/IP v4

Класс	Наименьший адрес	Наибольший адрес
A	1.0.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	129.0.0.0	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Специальные адреса: broadcast, multicast, loopback

В протоколе IP существует несколько соглашений об особой интерпретации IP-адресов:

- если IP-адрес состоит только из двоичных нулей:

0 0 0 0 ..... 0 0 0 0

то он обозначает адрес того узла, который сгенерировал этот пакет;

- если в поле номера сети стоят 0:

0 0 0 0 .....0 Номер узла

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:

1 1 1 1 .....1 1

то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник пакета. Такая рассылка называется ограниченным широковещательным сообщением (limited broadcast);

- если в поле адреса назначения стоят только 1:

Номер сети 1111.....11

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, то есть 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 IPv4 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 трафик пределами одной из составляющих общую сеть частей просто потому, что нет способа адресовать пакет одновременно всем узлам всех сетей составной сети.

Таким образом, в протоколе IPv4 применяется 32-разрядная адресация. На представление каждого адреса отводится четыре байта (в распространенной нотации они разделяются точками). Теоретически этого достаточно для адресации более чем 4 млрд. узлов. Однако необходимость одновременного предоставления некоторым пользователям не одного, а многих адресов значительно сужает эти рамки. Даже при условии оптимального использования каждого бита рано или поздно четырех миллиардов адресов окажется недостаточно. Широкое распространение мобильных устройств и перспективы подключения к глобальной сети основных устройств домашнего быта ставит необходимость увеличить емкость адресного пространства.

В качестве основных претендентов на новую версию протокола IP рассматривалось три разработки: TUBA (TCP and UDP with Bigger Addresses), CathIP (Common Architecture for the Internet) и SIPP (Simple Internet Protocol Plus). После их анализа был выработан новый проект, получивший название IPv6 (Internet Protocol version 6).

Основным отличием протокола IPv6 является система адресации. Он использует 128-разрядные адреса, что позволяет адресовать $3{,}40 \cdot 10^{38}$ узлов. Такой теоретический максимум практически недостижим даже при исключи-

тельно быстром развитии информационной техники и технологии.

Еще одним недостатком IPv4 является применяемый способ назначения адресов. Он не позволяет определить ни географическое положение, ни топологию сети, в которой находится узел. Вследствие этого в памяти магистральных маршрутизаторов интернета хранятся огромные объемы информации обо всех имеющихся адресах. В результате на маршрутизаторы ложится чрезмерная нагрузка, а их производительность существенно снижается.

Увеличение длины IP-адреса в протоколе IPv6 позволяет использовать больше уровней иерархии в системе адресации и ввести несколько различных типов адресов. Таким образом появляется возможность создать систему адресов со строгой иерархией. Крупным провайдерам будут выделяться большие блоки адресов. Провайдеры предоставляют блоки меньшего размера своим абонентам, которые, в свою очередь, распределяют их между подразделениями или отдельными пользователями.

При такой иерархической схеме адресации IPv6 каждому крупному блоку адресов соответствует единая точка входа в таблице маршрутизации. Это существенно упрощает маршрутизацию, поскольку для определения конечной точки следования пакета достаточно просмотреть относительно немного адресов. Кроме того, иерархическая модель позволяет уменьшить сложность и снизить стоимость маршрутизаторов сети.

1.17. Формат пакетов в протоколах IPv4 и IPv6

Основу транспортных средств стека протоколов TCP/IP представляет собой протокол IP. Основные функции протокола IP:

- перенос между сетями различных типов адресной информации в унифицированной форме;
- сборка и разборка пакетов при передаче их между сетями с различным максимальным значением длины пакета.

IP пакет протокола IPv4 состоит из заголовка и поля данных. Поля заголовка представлены в таблице 10.

Максимальная длина поля данных пакета ограничена разрядностью поля, определяющего эту величину, и составляет 65535 байтов, однако при передаче по сетям различного типа длина пакета выбирается с учетом максимальной длины пакета протокола нижнего уровня, несущего IP-пакеты. Если это кадры Ethernet, то выбираются пакеты с максимальной длиной в 1500

байтов, умещающиеся в поле данных кадра Ethernet.

В IPv6 поддерживаются усовершенствованные заголовки пакетов, значительно отличающиеся от заголовков пакетов IPv4. Переменная длина заголовков пакетов IPv4 создает трудности для маршрутизатора, вынужденного просматривать больший объем информации, чем это действительно необходимо для продвижения пакета. Заголовки пакетов IPv6 имеют фиксированную длину, равную 24 байтам.

Чтобы максимально упростить структуру заголовка, необходимая в первую очередь информация (например, адреса источника и получателя) включается в стандартный заголовок IPv6, при этом одно из его полей определяет, что именно находится дальше, – собственно данные или еще одна порция служебных сведений.

Таблица 10. Структура заголовка пакета IPv4

Название поля	**Размер, байт**	**Назначение**
Номер версии (**VERS**)	1/2	Указывает версию протокола IP
Длина заголовка (**HLEN**)	1/2	Задает значение длины заголовка измеренное в 32-битовых словах. Обычная длина заголовка 20 байт (5 32-битных слов), но при увеличении объема служебной информации длина может быть увеличена за счет дополнительных байтов в поле Резерв (IP OPTIONS)
Тип сервиса (**SERVICE TYPE**)	1	Задает приоритетность пакета и вид критерия выбора маршрута. Первые три бита этого поля образуют подполе приоритета пакета (PRECEDENCE). Приоритет может иметь значения от 0 (нормальный пакет) до 7 (пакет управляющей информации). Маршрутизаторы и компьютеры могут принимать во внимание приоритет пакета и обрабатывать более важные пакеты в первую очередь. Поле Тип сервиса содержит также три бита, определяющие критерий выбора маршрута. Установленный бит D (delay) говорит о том, что маршрут должен выбираться для минимизации задержки доставки данного пакета, бит T – для максимизации пропускной способности, а бит R – для максимизации надежности доставки.
Общая длина (**TOTAL LENGTH**)	2	Определяет общую длину пакета с учетом заголовка и поля данных.
Идентификатор пакета (**IDENTIFICATION**)	2	Используется для распознавания пакетов, образованных путем фрагментации исходного пакета. Все фрагменты должны иметь одинаковое значение этого поля.

Название поля	Размер, байт	Назначение
Флаги (**FLAGS**)	3/8	Указывает на возможность фрагментации пакета (установленный бит DF – Do not Fragment запрещает маршрутизатору фрагментировать данный пакет, а также на то, является ли данный пакет промежуточным или последним фрагментом исходного пакета (установленный бит MF – More Fragments говорит о том, что пакет переносит промежуточный фрагмент).
Смещение фрагмента (**FRAGMENT OFFSET**)	13/8	Используется для указания в байтах смещения поля данных этого пакета от начала общего поля данных исходного пакета, подвергнутого фрагментации. Используется при сборке/разборке фрагментов пакетов при передачах их между сетями с различными величинами максимальной длины пакета.
Время жизни (**TIME TO LIVE**)	1	Определяет предельный срок, в течение которого пакет может перемещаться по сети. Время жизни пакета измеряется в секундах и задается источником передачи средствами протокола IP. На шлюзах и в других узлах сети по истечении каждой секунды из текущего времени жизни вычитается единица; единица вычитается также при каждой транзитной передаче (даже если не прошла секунда). При истечении времени жизни пакет аннулируется.
Идентификатор протокола верхнего уровня (**PROTOCOL**)	1	Указывает, какому протоколу верхнего уровня принадлежит пакет (TCP, UDP, RIP)
Контрольная сумма (**HEADER CHECKSUM**)	2	Рассчитывается по всему заголовку.
Адрес источника (**SOURCE IP ADDRESS**)	4	Указывает адрес источника.
Адрес назначения (**DESTINATION IP ADDRESS**)	4	Указывает адрес назначения.
Резерв (**IP OPTIONS**)	–	Является необязательным и используется обычно только при отладке сети. Это поле состоит из нескольких фрагментов, каждый из которых может быть одного из восьми предопределенных типов. В этих фрагментах можно указывать точный маршрут прохождения маршрутизаторов, регистрировать проходимые пакетом маршрутизаторы, помещать данные системы безопасности, а также временные отметки. Так как число фрагментов может быть произвольным, то в конце поля Резерв должно быть добавлено несколько байт для выравнивания заголовка пакета по 32-битной границе.

Базовый заголовок протокола IPv6 состоит из нескольких полей. Для уменьшения времени, необходимого на пересылку и обработку пакетов, многие из них являются необязательными и используются только при необходимости. На рис. 22 представлена структура заголовка пакета IPv6.

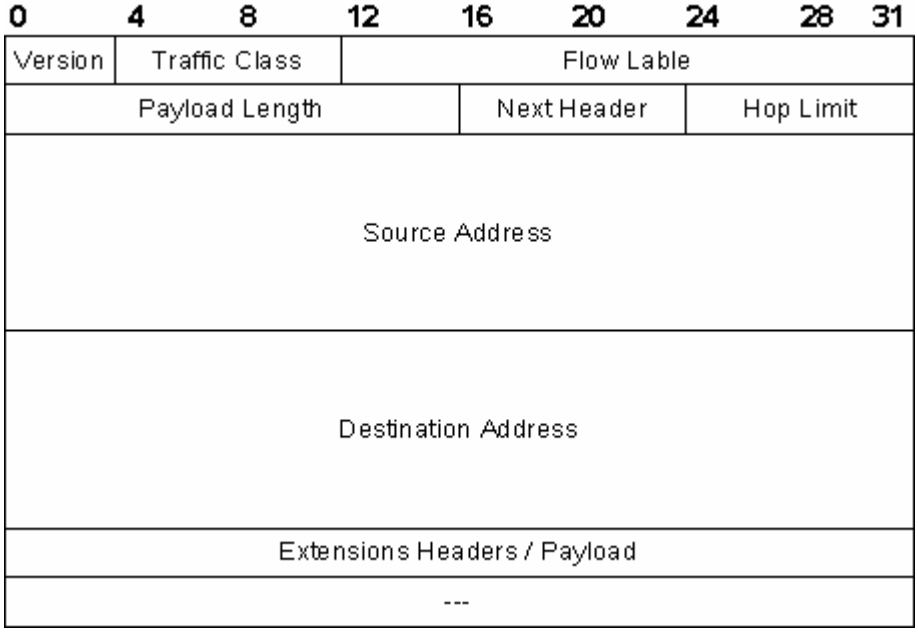


Рис. 22. Структура заголовка пакета IPv6.

Выделяются следующие структурные элементы заголовка:

- *Version* (4 бита) – версия протокола, для IPv6 имеет значение 6;
- *Traffic class* (8 бит). Аналог значения Type of service в протоколе IPv4. Поле предназначено для определения типа пересылаемого трафика, по которому определяется уровень качества услуг, необходимый для обработки данного пакета. Заполняется в соответствии со стандартом RFC-2474;
- *Flow label* (20 бит). Это так называемая метка потока. Она нужна для идентификации всех пакетов, принадлежащих одному потоку. Используется для того, чтобы промежуточные маршрутизаторы одинаково обрабатывали все данные с одной меткой;
- *Payload length* (16 бит). В этом поле указывается длина всего пакета за исключением базового заголовка IPv6. Измерение идет в октетах;
- *Next header* (8 бит). Указывает на тип следующего заголовка в соответствии со стандартом RFC-1700, который следует непосредственно за базовым. Это может быть как один из расширенных заголовков IPv6, так и заголовок протокола верхнего уровня (TCP, UDP и так далее);
- *Hop limit* (8 бит). В этом поле устанавливается так называемое максимальное число шагов. Первоначально в нем записывается определенное число.

Каждый маршрутизатор, через который проходит пакет, уменьшает его на единицу. Если значение в Hop limit достигнет нуля, пакет будет удален;

- *Source address* (128 бит) – адрес отправителя пакета в соответствии со стандартом RFC-1884;
- *Destination address* (128 бит) – адрес получателя, причем не обязательно конечного. Если в пакете присутствует маршрутный заголовок, то в этом поле будет находиться адрес следующего узла.

В заголовках IPv6 дополнительных типов содержится информация о маршрутизации, защите (шифровании) и фрагментации. Каждый из заголовков тоже имеет поле «следующего блока», с помощью которого получатель определяет, каким образом следует интерпретировать очередную порцию – как данные или как следующий заголовок.

В протоколе IPv6 имеется механизм, предусматривающий дальнейшее расширение. В IPv4 механизмы для реализации дополнительных средств, работающих на уровне протокола (например, процедуры шифрования), отсутствуют. В принципе, эта задача решается при помощи дополнительных протоколов, но такой подход усложняет работу устройств и снижает производительность. Поэтому уже в ходе проектирования IPv6 группа IETF[68] постаралась предусмотреть все необходимое для встраивания новых функций без глобальной переработки протоколов.

1.18. Требования, предъявляемые к вычислительным сетям

Главным требованием, предъявляемым к сетям, является выполнение основной функции – обеспечение возможности доступа к разделяемым ресурсам всех компьютеров, объединенных в сеть.

Все остальные требования – производительность, надежность, совместимость, управляемость, защищенность, расширяемость и масштабируемость – связаны с качеством выполнения основной задачи.

Хотя все эти требования весьма важны, часто QoS компьютерной сети трактуется более узко – в него включаются только две характеристики сети – производительность и надежность. В случае практической реализации в Win-

[68] IETF – Internet engineering task force, инженерная группа по развитию интернета. Одна из групп IAB, отвечающая за решение инженерных задач в интернете, выпускает большинство рекомендаций, используемых производителями для внедрения стандартов в архитектуру TCP/IP.

dows XP служба QoS устанавливается автоматически (рис. 23). При этом стандартные настройки таковы, что QoS резервирует под свои нужды 20% пропускной способности. Эту службу удалить нельзя, но можно ограничить резервируемую пропускную способность до 0%.

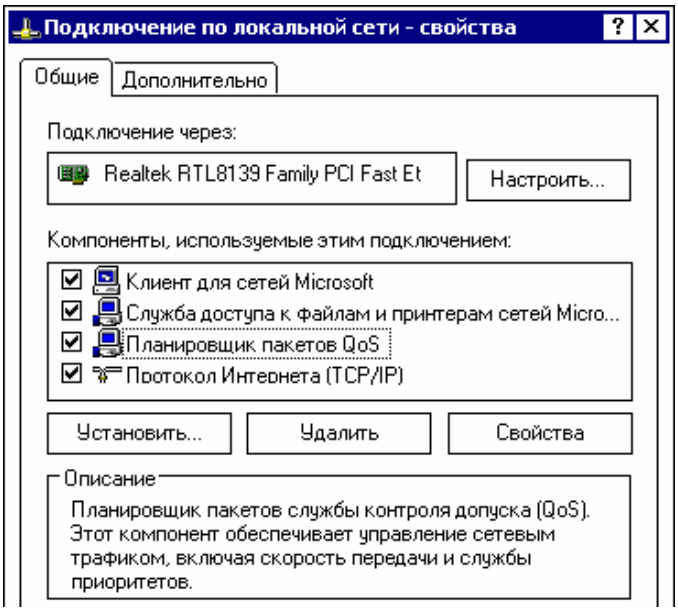


Рис. 23. Служба QoS среди других сетевых компонентов.

Независимо от выбранного показателя качества обслуживания сети, существуют два подхода к его обеспечению.

Первый подход состоит в том, что сеть гарантирует пользователю соблюдение некоторой числовой величины показателя качества обслуживания. Технологии frame relay и ATM позволяют строить сети, гарантирующие качество обслуживания по производительности.

Второй подход состоит в том, что сеть обслуживает пользователей в соответствии с их приоритетами. То есть качество обслуживания зависит от степени привилегированности пользователя или группы пользователей, к которой он принадлежит. Качество обслуживания в этом случае не гарантируется, а гарантируется только уровень привилегий пользователя. Такое обслуживание называется обслуживанием *best effort* – с наибольшим старанием. Сеть старается по возможности более качественно обслужить пользователя, но ничего при этом не гарантирует.

Производительность

Потенциально высокая производительность – это одно из основных свойств распределенных систем, к которым относятся компьютерные сети.

Оно обеспечивается возможностью распараллеливания работ между несколькими компьютерами сети. К сожалению, эту возможность не всегда удается реализовать. Выделяют следующие основные характеристики производительности сети:

- время реакции;
- пропускная способность;
- задержка передачи и вариация задержки передачи.

Время реакции сети является интегральной характеристикой производительности сети с точки зрения пользователя. В общем случае оно определяется как интервал времени между возникновением запроса пользователя к какой-либо сетевой службе и получением ответа на запрос. Знание сетевых составляющих времени реакции дает возможность оценить производительность отдельных элементов сети, выявить узкие места и в случае необходимости выполнить модернизацию сети для повышения ее общей производительности.

Пропускная способность отражает объем данных, переданных сетью или ее частью в единицу времени. Она характеризует скорость выполнения внутренних операций сети – передачи пакетов данных между узлами сети через различные коммуникационные устройства, то есть является непосредственной характеристикой качества выполнения основной функции сети. Поэтому пропускная способность чаще используется при анализе производительности сети, чем время реакции.

Пропускная способность измеряется либо в битах в секунду, либо в пакетах в секунду. Пропускная способность может быть мгновенной, максимальной и средней.

Средняя пропускная способность вычисляется делением общего объема переданных данных на время их передачи, причем выбирается достаточно длительный промежуток времени – час, день или неделя.

Мгновенная пропускная способность отличается от средней тем, что для усреднения выбирается малый промежуток времени – от 1 мс до нескольких секунд.

Максимальная пропускная способность – наибольшая мгновенная пропускная способность, зафиксированная в течение периода наблюдения.

Иногда полезно оперировать с *общей пропускной способностью* сети, которая определяется как среднее количество информации, переданной между всеми узлами сети в единицу времени. Этот показатель характеризует ка-

чество сети в целом, не дифференцируя его по отдельным сегментам или устройствам.

Важно отметить, что из-за последовательного характера передачи пакетов различными элементами сети *общая пропускная способность сети любого составного пути в сети будет равна минимальной* из пропускных способностей составляющих элементов маршрута. Для повышения пропускной способности составного пути необходимо в первую очередь обратить внимание на самые медленные элементы.

Задержка передачи определяется как задержка между моментом поступления пакета на вход какого-либо сетевого устройства или части сети и моментом появления его на выходе этого устройства. Этот параметр производительности по смыслу близок ко времени реакции сети, но отличается тем, что всегда характеризует только сетевые этапы обработки данных, без задержек обработки компьютерами сети. Обычно качество сети характеризуют величиной *максимальной задержки передачи*.

Пропускная способность и задержка передачи являются независимыми параметрами, так что сеть может обладать, например, высокой пропускной способностью, но вносить значительные задержки при передаче каждого пакета. Пример такой ситуации дает канал связи, образованный геостационарным спутником. Пропускная способность этого канала может быть весьма высокой, в то время как задержка передачи всегда составляет не менее 0,24 с, что определяется скоростью распространения сигнала (около 300 000 км/с) и длиной канала (72 000 км).

Надежность и безопасность

Важно различать несколько аспектов надежности. Для технических устройств используются такие показатели, как среднее время наработки на отказ, вероятность отказа, интенсивность отказов. Однако они пригодны для оценки надежности простых элементов и устройств, способных находиться только в двух состояниях – работоспособном или неработоспособном. Сложные системы, состоящие из многих элементов, кроме состояний работоспособности и неработоспособности, могут иметь другие промежуточные состояния, которые этими характеристиками не учитываются. Поэтому для оценки надежности сложных систем применяется другой набор характеристик.

Коэффициент готовности (availability) означает долю времени, в те-

чение которого система может быть использована. Готовность может быть улучшена путем введения избыточности в структуру системы: ключевые элементы системы должны существовать в нескольких экземплярах, чтобы при отказе одного из них функционирование системы обеспечивали другие.

Чтобы систему можно было отнести к высоконадежным, она должна обладать высокой готовностью и обеспечивать *сохранность данных* и защиту их от искажений.

Так как сеть работает на основе механизма передачи пакетов между конечными узлами, то одним из характерных показателей надежности является *вероятность доставки пакета* узлу назначения без искажений. Наряду с этим показателем могут использоваться и другие, например: *вероятность потери пакета*.

Другим аспектом надежности является *отказоустойчивость (fault tolerance)*. В сетях под отказоустойчивостью понимается способность системы скрыть от пользователя отказ отдельных ее элементов.

Еще одной характеристикой общей надежности является *безопасность (security)*, то есть способность системы защитить данные от несанкционированного доступа. В распределенной системе это сделать сложнее, чем в централизованной.

Расширяемость и масштабируемость

Термины расширяемость и масштабируемость иногда используют как синонимы, но это неверно – каждый из них имеет четко определенное самостоятельное значение.

Расширяемость (extensibility) означает возможность сравнительно легкого добавления отдельных элементов сети (пользователей, компьютеров, приложений, служб), наращивания длины сегментов сети и замены существующей аппаратуры на более мощную. При этом принципиально важно, что легкость расширения системы иногда может обеспечиваться в некоторых весьма ограниченных пределах. Например, локальная сеть Ethernet, построенная на основе одного сегмента толстого коаксиального кабеля, обладает хорошей расширяемостью, поскольку позволяет легко подключать новые станции. Однако она имеет ограничение на число станций – их число не должно превышать 30–40. Хотя сеть допускает физическое подключение к сегменту и большего числа станций (до 100), при этом чаще всего резко сни-

жается производительность сети. Наличие такого ограничения является признаком плохой масштабируемости системы при хорошей расширяемости.

Масштабируемость (scalability) означает, что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается или ухудшается очень незначительно. Для обеспечения масштабируемости сети приходится применять дополнительное коммуникационное оборудование и специальным образом структурировать сеть. Например, хорошей масштабируемостью обладает *многосегментная сеть*, построенная с использованием коммутаторов и маршрутизаторов и имеющая иерархическую структуру связей. Такая сеть может включать несколько тысяч компьютеров и при этом обеспечивать каждому пользователю сети нужное качество обслуживания.

Прозрачность

Прозрачность (transparency) – свойство сети скрывать от пользователя детали своего устройства. Прозрачность сети достигается в том случае, когда сеть представляется пользователям не как множество отдельных компьютеров, связанных между собой сложной системой кабелей, а как компьютер с системой разделения времени.

Прозрачность может быть достигнута на нескольких уровнях. На уровне пользователя прозрачность означает, что для работы с удаленными ресурсами пользователь использует те же команды и процедуры, что и для работы с локальными ресурсами. На программном уровне прозрачность заключается в том, что приложению для доступа к удаленным ресурсам требуются те же вызовы, что и для доступа к локальным ресурсам. Такая прозрачность требует сокрытия всех деталей распределенности средствами сетевой операционной системы.

Поддержка разных видов трафика

Компьютерные сети изначально предназначены для совместного доступа пользователя к ресурсам компьютеров: файлам, принтерам и т. п. Трафик, создаваемый традиционными службами компьютерных сетей, имеет свои особенности и существенно отличается от трафика сообщений в телефонных сетях или, например, в сетях кабельного телевидения. Однако 90-е годы стали годами проникновения в компьютерные сети трафика мультимедийных дан-

ных, представляющих в цифровой форме речь и видеоизображение. Компьютерные сети стали использоваться для организации видеоконференций, обучения и развлечения на основе видеофильмов и т. п. Естественно, что для динамической передачи мультимедийного трафика требуются иные алгоритмы и протоколы и, соответственно, другое оборудование. Следует отметить, что доля мультимедийного трафика с каждым годом увеличивается.

Главной особенностью трафика, образующегося при динамической передаче голоса или изображения, является наличие жестких требований к синхронности передаваемых сообщений. Для качественного воспроизведения непрерывных процессов, которыми являются звуковые колебания или изменения интенсивности света в видеоизображении, необходимо получение измеренных и закодированных амплитуд сигналов с той же частотой, с которой они были измерены на передающей стороне. При запаздывании сообщений будут наблюдаться искажения. Напротив, трафик компьютерных данных характеризуется крайне неравномерной интенсивностью поступления сообщений в сеть при отсутствии жестких требований к синхронности доставки этих сообщений.

Все первоначальные алгоритмы компьютерной связи, протоколы и коммуникационное оборудование были рассчитаны именно на пульсирующий трафик, поэтому необходимость передавать мультимедийный трафик потребовала принципиальных изменений как в протоколах, так и оборудовании. Сегодня практически все новые протоколы в той или иной степени предоставляют поддержку мультимедийного трафика.

Особую сложность представляет совмещение в одной сети традиционного компьютерного и мультимедийного трафика. Передача исключительно мультимедийного трафика компьютерной сетью связана с определенными сложностями, но вызывает меньшие трудности. А вот случай сосуществования двух типов трафика с противоположными требованиями к качеству обслуживания является значительно более сложной задачей. Обычно протоколы и оборудование компьютерных сетей относят мультимедийный трафик к второстепенному, поэтому качество его обслуживания оставляет желать лучшего. Сегодня затрачиваются большие усилия по созданию сетей, которые не ущемляют интересы одного из типов трафика. Наиболее близки к этой цели сети на основе технологии ATM, разработчики которой изначально учитывали случай сосуществования разных типов трафика в одной сети.

Управляемость

Управляемость сети подразумевает возможность централизованно контролировать состояние основных элементов сети, выявлять и разрешать проблемы, возникающие при ее работе, выполнять анализ производительности и планировать развитие. В идеале средства управления сетями представляют собой систему, осуществляющую наблюдение, контроль и управление каждым элементом сети – от простейших до самых сложных устройств, при сеть рассматривается как единое целое, а не как разрозненный набор отдельных устройств.

Совместимость

Совместимость или *интегрируемость* означает, что сеть способна включать в себя самое разнообразное программное и аппаратное обеспечение, то есть в ней могут сосуществовать различные операционные системы, поддерживающие разные стеки коммуникационных протоколов, и работать аппаратные средства и приложения от разных производителей. Сеть, состоящая из разнотипных элементов, называется неоднородной или *гетерогенной*, а если гетерогенная сеть работает без проблем, то она является *интегрированной*. Основной путь построения интегрированных сетей – использование модулей, выполненных в соответствии с открытыми стандартами и спецификациями.

1.19. Классификация сетей

Для классификации компьютерных сетей используются различные признаки, приведенные на рис. 24.

Классификация по технологии передачи

Есть два основных типа технологий передачи, используемые в сетях:

- *вещание* (от одного ко многим);
- *точка-точка*.

Сети вещательного типа имеют единый канал передачи данных, который используют все машины сети. Короткое сообщение, называемое *пакет*, имеющее специальную структуру, отправленное какой-то машиной, получают все другие машины сети. В определенном поле пакета указан адрес получателя. Каждая машина проверяет это поле. Если она обнаруживает в этом

поле свой адрес, то она приступает к обработке этого пакета, если в этом поле не ее адрес, то она просто игнорирует этот пакет.

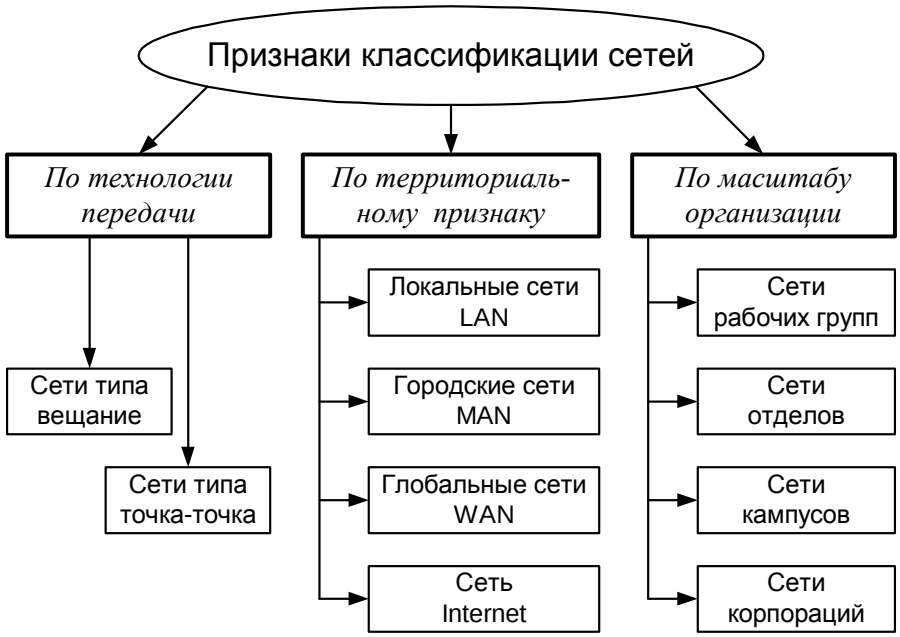


Рис. 24. Классификация сетей.

Вещательные сети, как правило, имеют *режим широкого вещания* – когда один пакет адресуется всем машинам в сети. Есть также *режим группового вещания*: один и тот же пакет получают машины, принадлежащие к определенной группе в сети. Вещательные сети используются на географически небольших территориях.

Сети точка–точка соединяют каждую пару машин индивидуальными каналом. Поэтому прежде, чем пакет достигнет адресата, он проходит через несколько промежуточных хостов. В таких сетях возникает потребность в маршрутизации пакетов. От ее эффективности зависит скорость доставки сообщений, распределение нагрузки в сети. Сети точка-точка используются при построении крупных сетей, охватывающих большие регионы.

Классификация по территориальному признаку

К *локальным сетям*[69] относят сети компьютеров, сосредоточенные на небольшой территории (обычно в радиусе не более 1–2 км). В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации. Из-за коротких расстояний в локальных сетях имеется возможность использования дорогих высококачественных линий

[69] LAN – Local area networks.

связи, которые позволяют, применяя простые методы передачи данных, достигать высоких скоростей обмена данными порядка 100 и даже 1000 Мбит/с. В связи с этим услуги, предоставляемые локальными сетями, отличаются широким разнообразием и обычно предусматривают реализацию в режиме *online*[70].

Городские сети (или сети мегаполисов[71] появились сравнительно недавно. Они предназначены для обслуживания территории крупного города – мегаполиса.

При достаточно больших расстояниях между узлами (десятки километров) MAN обладают качественными линиями связи и высокими скоростями обмена, иногда даже более высокими, чем в классических локальных сетях. Как и в случае локальных сетей, при построении MAN уже существующие линии связи не используются, а прокладываются заново.

В то время как локальные сети наилучшим образом подходят для разделения ресурсов на коротких расстояниях и широковещательных передач, а глобальные сети обеспечивают работу на больших расстояниях, но с ограниченной скоростью и небогатым набором услуг, сети мегаполисов занимают промежуточное положение. Они используют цифровые магистральные линии связи, часто оптоволоконные, со скоростями от 45 Мбит/с, и предназначены для связи локальных сетей в масштабах города и соединения локальных сетей с глобальными. Первоначально разработанные для передачи данных, сейчас они поддерживают и такие услуги, как видеоконференции и интегральную передачу голоса и текста. Развитие технологии сетей мегаполисов осуществляется местными телефонными компаниями. Исторически сложилось так, что телефонные компании всегда обладали слабыми техническими возможностями, и из-за этого не могли привлечь крупных клиентов. Чтобы преодолеть свою отсталость, местные предприятия связи занялись разработкой сетей на основе современных технологий. Сети мегаполисов являются общественными сетями, поэтому их услуги обходятся дешевле, чем построение собственной (частной) сети в пределах города.

---

[70] Online – «находящийся в состоянии подключения». Используется в отношении коммуникационного оборудования для указания на режим связи. В отношении программного обеспечения почти всегда означает «подключенный к интернету» или «функционирующий только при подключении к интернету». Еще одно значение слова – «происходящее в интернете», «существующее в интернете».

[71] MAN – Metropolitan area networks.

На сегодняшний день в России наиболее быстро идет развитие сети мегаполиса в г. Москве за счет расширения и интеграции сетей крупных провайдеров связи – МТУ, Корбина и т.д. Подобные же процессы протекают и в других крупных городах – Ростове-на-Дону, Краснодаре, Санкт-Петербурге. Для развития сетей мегаполисов необходимо выполнение нескольких условий: высокий уровень доходов населения, широкое распространение домашних компьютеров, тенденция к быстрому росту числа пользователей интернета и локальных сетей и т. д. К сожалению, во многих городах эти условия не реализуются.

Региональные сети[72] и *глобальные сети*[73] объединяют территориально рассредоточенные компьютеры, которые могут находиться в различных городах и странах на расстоянии сотен и тысяч километров. Прокладка высококачественных линий связи на большие расстояния обходится очень дорого, поэтому в глобальных сетях часто используются уже существующие линии связи, изначально предназначенные совсем для других целей. Например, многие глобальные сети строятся на основе телефонных и телеграфных каналов общего назначения.

Из-за низких скоростей таких линий связи в глобальных сетях (десятки килобит в секунду) набор предоставляемых услуг обычно ограничивается передачей файлов, преимущественно не в оперативном, а в фоновом режиме, с использованием электронной почты. Для устойчивой передачи дискретных данных по некачественным линиям связи применяются методы и оборудование, существенно отличающиеся от методов и оборудования, характерных для локальных сетей. Как правило, здесь применяются сложные процедуры контроля и восстановления данных, так как наиболее типичный режим передачи данных по территориальному каналу связи связан со значительными искажениями сигналов.

Отличия локальных сетей от глобальных

Протяженность, качество и способ прокладки линий связи. Класс локальных вычислительных сетей по определению отличается от класса глобальных сетей небольшим расстоянием между узлами сети. Это в принципе делает возможным использование в локальных сетях качественных линий

[72] WAN – Wide area networks.
[73] GAN – Global area networks.

связи: коаксиального кабеля, витой пары, оптоволоконного кабеля.

Сложность методов передачи и оборудования. В условиях низкой надежности физических каналов в глобальных сетях требуются более сложные, чем в локальных сетях, методы передачи данных и соответствующее оборудование. Так, в глобальных сетях широко применяются модуляция, асинхронные методы, сложные методы контрольного суммирования, квитирование и повторные передачи искаженных кадров. С другой стороны, качественные линии связи в локальных сетях позволили упростить процедуры передачи данных за счет применения немодулированных сигналов и отказа от обязательного подтверждения получения пакета.

Скорость обмена данными. Одним из главных отличий локальных сетей от глобальных является наличие высокоскоростных каналов обмена данными между компьютерами, скорость которых (10, 100 и 1000 Мбит/с) сравнима со скоростями работы устройств и узлов компьютера – дисков, внутренних шин обмена данными и т. п. За счет этого у пользователя локальной сети, подключенного к удаленному разделяемому ресурсу (например, диску сервера), складывается впечатление, что он пользуется этим диском, как «своим». Для глобальных сетей типичны гораздо более низкие скорости передачи данных – 2-64 Кбит/с, на магистральных каналах – до 2 Мбит/с.

Оперативность выполнения запросов. Время прохождения пакета через локальную сеть обычно составляет несколько миллисекунд, время же его передачи через глобальную сеть может достигать нескольких секунд. Низкая скорость передачи данных в глобальных сетях затрудняет реализацию служб для режима online, который является обычным для локальных сетей.

Разнообразие услуг. Локальные сети предоставляют, как правило, широкий набор услуг – это различные виды услуг файловой службы, услуги печати, услуги службы передачи факсимильных сообщений, услуги баз данных, электронная почта и другие, в то время как глобальные сети в основном предоставляют почтовые услуги и иногда файловые услуги с ограниченными возможностями – передачу файлов из публичных архивов удаленных серверов без предварительного просмотра их содержания.

Разделение каналов. В локальных сетях каналы связи используются, как правило, совместно сразу несколькими узлами сети, а в глобальных сетях – индивидуально.

Использование метода коммутации пакетов. Важной особенностью локальных сетей является неравномерное распределение нагрузки. Отношение пиковой нагрузки к средней может составлять 100:1 и выше. Такой трафик называют *пульсирующим*. Из-за этой особенности трафика в локальных сетях для связи узлов применяется метод коммутации пакетов, который для пульсирующего трафика оказывается гораздо более эффективным, чем традиционный для глобальных сетей метод коммутации каналов. Эффективность метода коммутации пакетов состоит в том, что сеть в целом передает в единицу времени больше данных своих абонентов. В глобальных сетях метод коммутации пакетов также используется, но наряду с ним часто применяется и метод коммутации каналов, а также некоммутируемые каналы – как унаследованные технологии некомпьютерных сетей.

Масштабируемость. Локальные сети обладают плохой масштабируемостью из-за жесткости базовых топологий, определяющих способ подключения станций и длину линии. При использовании многих базовых топологий характеристики сети резко ухудшаются при достижении определенного предела по количеству узлов или протяженности линий связи. Глобальным же сетям присуща хорошая масштабируемость, так как они изначально разрабатывались в расчете на работу с произвольными топологиями.

Классификация по масштабу организации

Еще одним способом классификации сетей является их *классификация по масштабу* производственного подразделения, в пределах которого действует сеть. Различают сети отделов, сети кампусов и корпоративные сети.

Сети рабочих групп. К таким сетям относят совсем небольшие сети, включающие до 10–20 компьютеров, Характеристики сетей рабочих групп практически не отличаются от описанных выше характеристик сетей отделов. Такие свойства, как простота сети и однородность, здесь проявляются в наибольшей степени.

Сети отделов – это сети, которые используются сравнительно небольшой группой сотрудников, работающих в одном отделе предприятия. Эти сотрудники решают некоторые общие задачи, например ведут бухгалтерский учет или занимаются маркетингом. Считается, что отдел может насчитывать до 100–150 сотрудников.

Главной целью сети отдела является разделение локальных ресурсов, таких как приложения, данные, лазерные принтеры и модемы. Обычно сети отделов имеют один или два файловых сервера и не более тридцати пользователей. В них локализуется большая часть трафика предприятия. Для такой сети характерен один или два типа операционных систем. Чаще всего – это сеть с выделенным сервером.

Сети кампусов получили свое название от английского слова *campus* – студенческий городок. Именно на территории университетских городков часто возникала необходимость объединения нескольких мелких сетей в одну большую сеть. Сейчас это название не связывают со студенческими городками, а используют для обозначения сетей любых предприятий и организаций, распределенных по достаточно большой, но единой территории. Глобальные соединения в сетях кампусов не используются. Службы сети включают взаимодействие между отделами, доступ к общим базам данных предприятия, высокоскоростным модемам и принтерам. В результате сотрудники каждого отдела предприятия получают доступ к некоторым файлам и ресурсам сетей других отделов.

Важнейшей службой, предоставляемой сетями кампусов, является доступ к корпоративным базам данных независимо от того, на каких типах компьютеров они располагаются.

Именно на уровне сети кампуса возникают проблемы интеграции неоднородного аппаратного и программного обеспечения. Типы компьютеров, сетевых операционных систем, сетевого аппаратного обеспечения могут отличаться в каждом отделе. Отсюда вытекают сложности управления сетями кампусов. Администраторы должны быть в этом случае более квалифицированными, а средства оперативного управления сетью – более совершенными по сравнению с администраторами обычных локальных сетей.

Корпоративные сети (*intranet*) объединяют большое количество компьютеров на всех территориях отдельного предприятия, даже если они сильно разобщены по территории. Для корпоративной сети характерны:

- *масштабность* – тысячи пользовательских компьютеров, сотни серверов, огромные объемы хранимых и передаваемых по линиям связи данных, множество разнообразных приложений;
- *высокая степень гетерогенности* – типы компьютеров, коммуникационного оборудования, операционных систем и приложений различны;

- *использование глобальных связей* – сети филиалов соединяются с помощью телекоммуникационных средств, в том числе телефонных каналов, радиоканалов, спутниковой связи.

1.20. Начальные сведения о глобальных сетях

Хотя в основе локальных и глобальных вычислительных сетей лежит один и тот же метод – метод коммутации пакетов (кадров, ячеек), глобальные сети имеют достаточно много отличий от локальных сетей. Эти отличия касаются как принципов работы (например, принципы маршрутизации почти во всех типах глобальных сетей, кроме сетей TCP/IP, основаны на предварительном образовании виртуального канала), так и терминологии.

Глобальные вычислительные сети обычно работают в режиме коммутации пакетов, наиболее подходящем для компьютерного трафика, что следует из данных о суммарном трафике, передаваемом сетью в единицу времени и из стоимости услуг такой территориальной сети. Обычно при равенстве предоставляемой скорости доступа сеть с коммутацией пакетов оказывается в 2-3 раза дешевле сети с коммутацией каналов (телефонной сети).

С другой стороны, более распространены и доступны услуги, предоставляемые телефонными сетями или первичными сетями, поддерживающими услуги выделенных каналов.

В зависимости от того, какие компоненты взяты в аренду, принято различать корпоративные сети, построенные с использованием:

- выделенных каналов;
- коммутации каналов;
- коммутации пакетов.

Территориальные сети, используемые для построения корпоративной сети, целесообразно делить на две большие категории:

- магистральные сети;
- сети доступа.

Магистральные территориальные сети (backbone wide-area networks) используются для образования одноуровневых связей между крупными локальными сетями, принадлежащими большим подразделениям предприятия. Обычно в качестве магистральных сетей используются цифровые выделенные каналы со скоростями от 2 до 622 Мбит/с (по которым передается трафик IP), сети с коммутацией пакетов frame relay, ATM, X.25 или TCP/IP.

Под *сетями доступа* понимаются территориальные сети, необходимые для связи небольших локальных сетей и отдельных удаленных компьютеров с центральной локальной сетью предприятия.

В качестве отдельных удаленных узлов могут выступать, например, терминалы в удаленных филиалах предприятия, датчики *телеметрии* на удаленном объекте, банкоматы или кассовые аппараты и т.д. Банкоматы или кассовые аппараты обычно рассчитаны на взаимодействие с центральным компьютером по сети X.25, которая в свое время специально разрабатывалась как сеть для удаленного доступа терминального оборудования к центральному компьютеру.

В качестве сетей доступа часто применяются телефонные аналоговые сети и сети ISDN. При подключении локальных сетей филиалов также используются выделенные каналы со скоростями от 19,2 до 128 Кбит/с.

Программные и аппаратные средства, обеспечивающие подключение компьютеров или локальных сетей удаленных пользователей к корпоративной сети, называются *средствами удаленного доступа*. Обычно на клиентской стороне эти средства представлены модемом и соответствующим программным обеспечением.

Организацию удаленного доступа со стороны центральной локальной сети обеспечивает *сервер удаленного доступа*[74]. Сервер удаленного доступа представляет собой программно-аппаратный комплекс, совмещающий функции маршрутизатора, моста и шлюза. Сервер выполняет ту или иную функцию в зависимости от типа протокола, по которому работает удаленный пользователь или удаленная сеть.

Структура глобальной сети, используемой для объединения в корпоративную сеть отдельных локальных сетей и удаленных пользователей, достаточно типична. Она имеет ярко выраженную иерархию территориальных средств передачи данных, включающую высокоскоростную магистраль (например, каналы SDH 155-622 Мбит/с), более медленные территориальные сети доступа для подключения локальных сетей средних размеров (например, frame relay) и телефонную сеть общего назначения для удаленного доступа сотрудников.

[74] RAS – Remote access server.

1.21. Организация интернета

Семейство протоколов TCP/IP определяет структуру и порядок передачи данных по интернету и имеет несколько уровней.

Уровни взаимодействия	**Протоколы**
Прикладной	HTTP, DNS, POP3, IMAP4, SMTP, NNTP, FTP
Транспортный	TCP, UDP
Сетевой	IP
Канальный	PPP, Ethernet

Основная задача *канального уровня* – осуществление передачи информации потоком битов, которые организуются в виде кадров данных и передаются от компьютера к компьютеру.

Канальный уровень включает:

- физический уровень, на котором и организуется перенос информации от компьютера к компьютеру;
- канальный уровень, обеспечивающий формирование кадров данных.

Физический уровень занимает в любой сетевой архитектуре особое место, так как именно на нем происходит реальный перенос информации от компьютера к компьютеру. Физический уровень состоит из физических элементов, служащих непосредственно для передачи информации по каналам связи. К таковым относятся любая среда передачи данных, например, обычный телефонный провод, коаксиальный кабель, витая пара, оптоволокно, радиоэфир и др., а также специальная аппаратура, преобразующая сигнал из линии связи в компьютерную форму и наоборот. Это модем, сетевая карта, антенна и т.д.

Протоколы физического уровня определяются разработчиками соответствующего оборудования и зависят от особенностей используемой среды передачи и области применения.

Элементы физического уровня:

Среда передачи данных	**Аппаратура сопряжения**
Телефонный провод	Модем
Коаксиальный кабель, витая пара	Сетевая карта
Оптоволокно	Оптический трансивер
Радиоэфир	Антенна, радиопередатчик

На физическом уровне передача информации рассматривается как поток битов и измеряется в bps[75].

На *канальном уровне* рассматривается передача данных от компьютера к компьютеру в виде кадров данных. Кадром данных называют отформатированный поток битов, передаваемых на физическом уровне. Он состоит из следующих элементов:

- заголовок кадра, содержит 48-битный адрес получателя, 48-битный адрес отправителя, 16-битный указатель типа кадра
- биты данных
- 32-битная контрольная сумма для проверки целостности кадра.

При соединении компьютеров по телефонной или выделенной линии (соединение точка – точка) чаще всего применяются протоколы PPP[76]. Это целое семейство протоколов, в котором сам протокол PPP формирует кадры, передает тип кадра и обеспечивает его целостность.

Сетевой уровень обеспечивает доставку данных между любыми двумя узлами сети с произвольной топологией.

Основные задачи уровня:

- глобальная адресация, то есть присвоение глобальных адресов, не зависящих от локальных;
- маршрутизация, то есть определение путей доставки пакетов данных. Для решения этой задачи используется так называемая *таблица маршрутизации*, представляющая собой базу данных, в которой хранится и регулярно обновляется информация о сети. Таблица маршрутизации содержит список IP-адресов и IP-сетей с указанием, на какой интерфейс надо отправлять тот или иной IP-пакет;
- разбиение информации на пакеты для доставки через канальный уровень.

На *транспортном уровне* работает транспортный протокол – центральный протокол во всей иерархии. Именно он обеспечивает надежную передачу данных от одного абонента сети другому.

Основные задачи транспортного уровня:

---

[75] bps (bits per second – бит/сек) – единица измерения скорости при последовательной передаче данных.

[76] PPP – Point to point protocol, протокол точка–точка. Представляет собой механизм для создания и запуска IP и других сетевых протоколов на последовательных линиях связи.

- обеспечение связи между прикладными программами на сетевых компьютерах;
- восстановление исходной последовательности пакетов, переданных на сетевом уровне.

Адрес на транспортном уровне состоит из двух частей:

- сетевой адрес компьютера (IP адрес);
- номер порта[77] требуемой программы на сетевом компьютере.На *прикладном уровне* рассматривается взаимодействие прикладных программ. Наиболее часто употребляемыми являются следующие протоколы:
- DNS – доменная система имен, обеспечивает символическое представление адресов на сетевом уровне;
- протоколы электронной почты
- HTTP – протокол для работы с гипертекстовыми документами;
- FTP – протокол передачи файлов;
- TELNET – протокол эмуляции виртуального терминала;
- NNTP – протокол для передачи новостей.

Доменная система имен

Компьютеры IP-сетей обмениваются информацией, используя для опознания друг друга адреса – 4-байтные коды, которые для удобства принято представлять соответствующей комбинацией десятичных чисел. Например: **144.206.160.32**. В общем случае такие числовые адреса могут трактоваться по-разному, наиболее логичной представляется следующая:

<класс сети><номер сети><номер компьютера>

Такая комбинация подразумевает, что множество представимых числовых номеров делится на сети разного масштаба (см. также параграф 1.16). С помощью специального механизма (маскирования) любая сеть, в свою очередь, может быть представлена набором более мелких сетей. Локальная сеть организации может быть создана вообще с предоставлением ей только одно-

[77] Сетевой порт — параметр протоколов TCP и UDP, определяющий назначение пакетов данных, передаваемых на хост по сети. Это условное число от 1 до 65535, позволяющее различным программам, выполняемым на одном хосте, получать данные независимо друг от друга. Каждая программа обрабатывает данные, поступающие на определенный порт (иногда говорят, что программа «слушает» этот номер порта). Обычно за некоторыми распространенными сетевыми протоколами закреплены стандартные номера портов (например, веб-серверы обычно принимают данные по протоколу HTTP на TCP-порту 80)

го внешнего числового адреса. Хотя компьютеры внутри этой сети имеют адреса, уникальные в ее пределах.

Числовые адреса удобны для компьютеров, но не для пользователей. Поэтому в Интернет предусмотрена возможность использования их аналогов в текстовом представлении. Наличие двух представлений адресов приводит к необходимости их преобразования из одной формы в другую или наоборот. Это реализуется серверами доменной системы имен – DNS.

Доменная система имен – это метод назначения имен путем передачи сетевым группам ответственности за их подмножество имен. Появление DNS вызвано тем что цифровые IP-адреса неудобны для восприятия и запоминания человеком.

Каждый уровень системы называется доменом. Уровни разделяются точками и называются доменами первого, второго, третьего и т.д. уровней. В имени может быть до 255 доменов, но практически их редко бывает больше пяти. Домен может создавать или изменять подчиненные домены. В конкретных адресах представлено различное число доменов. Например, адрес, состоящий из четырех доменов, представляется следующим образом:

`domain4.domain3.domain2.domain1`

- *domain1* – двухбуквенный код страны или другой общемировой домен первого уровня;
- *domain2* – код города (при этом часто тяготеют к сокращению исходного названия, например, Kazan – kzn);
- *domain3* – наименование организации;
- *domain4* – имя компьютера.

Такая трактовка не обязательна, доменное имя конечного компьютера может содержать всего два доменных адреса. Например, rambler.ru.

Домены первого уровня[78] могут быть двух типов. Первый тип регулируется на основе стандарта ISO 3166[79] и привязан к государству, на территории которого располагаются подсети домена. Это двухбуквенный код страны, например: ru, us, de, fr, kr, hu, no, tw, jp и т.д. Для России действует также домен первого уровня su. Полный список национальных доменов приведен в

[78] TLD – Top level domains, домены верхнего (первого) уровня.

[79] ISO 3166 – международный стандарт ISO, определяющий кодовые обозначения государств и зависимых территорий, а также основных административных образований внутри государств.

приложении 1.

Второй тип доменов первого уровня ведет свое начало от сокращенных наименований составляющих сети NSFNET. Наименования следующие:

- *com* – коммерческие организации;
- *edu* – учебные и научные организации;
- *gov* – правительственные организации;
- *mil* – военные организации;
- *net* – сетевые организации разных сетей;
- *org* – другие организации.

Почти все сети в этих доменных зонах давно действуют по всему миру, без дополнительной информации зачастую невозможно определить, какой стране мира он соответствует.

Начиная с 1998 года доменные зоны первого уровня регистрируются после положительного решения заявок, поданных в ICANN[80]. В настоящее время доступно использование следующих доменов первого уровня:

- *aero* – для субъектов авиатранспортной индустрии;
- *biz* – для коммерческих организаций (в дополнение к домену *com*);
- *cat* – для использования каталанским языковым и культурным сообществом;
- *coop* – кооперативы;
- *edu* – высшие учебные заведения, признаваемые в качестве таковых Департаментом образования США;
- *info* – информационные ресурсы (без ограничений);
- *jobs* – кадровые агентства;
- *mobi* – для продавцов и поставщиков мобильного контента и услуг, связанных с мобильной связью;
- *museum* – музеи;
- *name* – физические лица;
- *pro* – сертифицированные профессионалы и смежные темы;
- *travel* – для субъектов туристического бизнеса.

[80] ICANN – Internet corporation for assigned names and numbers, Всемирная корпорация по присвоению доменных имен и номеров. Некоммерческая организация, учреждена в 1998 г. Министерством торговли США. Контролирует выдачу доменных имен верхнего уровня, отвечает за адресное пространство интернета, определение параметров протоколов, систему доменных имен и систему корневых серверов. До создания ICANN эти вопросы решали несколько не связанных между собою агентств.

Кроме того, существуют домены ограниченного использования:

- *int* – межгосударственные организации;
- *arpa* – инфраструктура интернета и, ранее, адреса в закрытой (военной) части сети Интернет США;
- *root* – домен прописан в корневых серверах DNS, контролируемых компанией Verisign, но его назначение никогда не комментировалось. По всей видимости он используется только для внутренних целей;

Устаревшие и неиспользуемые домены первого уровня:

- *nato* – структуры международной организации НАТО, в настоящее время не используется, по крайней мере, в публично доступной части сети интернета, откуда был удален в июле 1996 г.;
- *web* – домен, выделенный для использования частным коммерческим регистратором Image Online Design. В связи с протестами общественности корневые сервера этого домена подключены к общей системе DNS не были;
- *csnet* – домен, предназначенный для связи с CSNET. Перестал использоваться после объединения CSNET и BITNET (см. главу 2);
- *ddn* – домен верхнего уровня, предназначенный для использования в американской оборонной сети DDN. Был запланирован, но так и не реализован.

Согласно RFC 2606, следующие домены верхнего уровня зарезервированы для различных целей, при этом они никогда не использовались как реальные имена доменов в глобальной DNS:

- *example* – зарезервировано для примеров;
- *invalid* – зарезервировано для использования в очевидно неверных именах доменов;
- *localhost* – зарезервировано для того чтобы избежать конфликтов с традиционным использованием localhost[81];
- *test* – зарезервировано для использования в тестах;
- *local* – для адресов, применяемых в пределах одной машины или локальной компьютерной сети.

Кроме того, существуют общеупотребительные псевдодомены, которые не присутствовали в адресном пространстве DNS, но общеупотребимы при пересылке почты из Интернета в сети с другим способом адресации. Для обработки писем, отправляемых на адреса в этом домене, почтовое программное обеспечение на конкретной машине, через которую отправляется

[81] Localhost – обращение компьютера к самому себе.

почта, должно быть настроено соответствующим образом.

- *uucp* – для отправки почты на машины, доступные при помощи протокола UUCP[82];
- *bitnet* – для отправки почты в сеть BITNET;
- *fidonet* – для отправки почты в сеть FIDO.

В июне 2005 ICANN объявила об одобрении в принципе нескольких новых доменов, внедрение которых находится на разных стадиях реализации:

- *post* – почтовые службы;
- *xxx* – сайты «для взрослых». Руководство ICANN проголосовало против домена «xxx» девятью голосами против пяти. После этого вопрос о введении домена перешел в стадию судебного разбирательства между заинтересованными в его созданиями коммерческими структурами и правительственными инстанциями (прежде всего Министерством торговли) США;
- *asia*, *mail*, *tel* – находятся в стадии рассмотрения.

В настоящее время ICANN также приступила к рассмотрению предложений по внедрению доменов верхнего уровня на национальных языках – при этом уже поданные предложения вовсе не ограничиваются принципом «один язык – один домен». Так, поданные предложения по доменам первого уровня на персидском языке включают в себя 15 наименований разнообразного назначения.

Поддержка доменов верхнего уровня осуществляется при помощи *корневых серверов DNS*. Основные корневые серверы DNS обозначаются латинскими буквами от A до M. Они управляются различными организациями, действующими по согласованию с ICANN.

Теоретически кто угодно может установить и начать использовать собственные корневые серверы DNS. На практике в интернете периодически появляются различные группы лиц и организации, открывающие для публичного использования альтернативные корневые серверы DNS. Как правило, эти системы дополняют общепринятый набор доменов некоторым количеством новых доменов первого уровня, иногда – дополняют техническую реализацию. Например, до того, как DNS была расширена для возможности исполь-

[82] UUCP – Unix-to-Unix copy. Изначально – команда копирования файлов между двумя компьютерами под управлением операционной системы UNIX. Протокол UUCP фактически является ее расширением, позволяя копировать файлы с локальной машины на удаленную и наоборот.

зовать в доменных именах символы национальных алфавитов, было предпринято несколько попыток создать дополнительные системы DNS, с доменными именами, в том числе первого уровня, содержащими символы того или иного национального алфавита. Эти попытки не получили широкого распространения, хотя ряд таких проектов продолжает существовать до сих пор.

Дополнительные домены верхнего уровня могут использоваться специализированным программным обеспечением, как правило – в пределах одного компьютера, для перехвата и последующей обработки части обращений к Интернет. Например, домен *onion* используется программным обеспечением анонимной IP-сети Tor, для перехвата и последующей маршрутизации обращений к скрытым сервисам этой сети, а домен *i2p* – программным обеспечением анонимной IP-сети I2P.

Протоколы электронной почты

Электронная почта – наиболее широко используемое приложение в интернете. Она относится к асинхронному типу коммуникационных систем, т.к. после отправки электронное сообщение хранится в почтовом ящике получателя до тех пор, пока тот не войдет в систему и не прочитает его.

Сообщение электронной почты состоит из двух основных частей: заголовка и тела (основного текста) сообщения. Заголовок содержит различную служебную, такую как имя отправителя, сведения о нем, время отправки, информацию о программе-клиенте электронной почты и ее версии, сведения о почтовых серверах, через которые прошло письмо и т.д. Тело сообщения содержит собственно текст сообщения. В нем также может содержаться бинарный контент (картинка, аудиозапись, видеофайл, программа). Протокол пересылки электронной почты допускает передачу только текстовых символов ASCII. Поэтому двоичные файлы перед передачей кодируются в специальном формате.

Для отправки сообщений используется протокол SMTP. Для получения используются протоколы POP3 и IMAP4. Прием и отправка почты совершенно независимы. Например, размер письма, которое отправляет абонент, никоим образом не зависит от размера его почтового ящика, поскольку письмо при отправке не попадает в его почтовый ящик.

Надо уметь четко различать назначение серверов входящей и исходящей почты. С сервера входящей почты происходит прием почты, с сервера исхо-

дящей – отправка. Это два совершенно разных сервера, хотя они могут быть установлены на одном и том же компьютере и иметь одно доменное имя.

Различные неудобства связаны с тем, что часто человеку приходится работать с почтой с разных компьютеров. С помощью POP3 клиент может получить доступ к сообщению на сервере электронной почты. Но когда сообщение передается клиенту, с сервера оно удаляется. Это не всегда удобно, так как зачастую приходиться обращаться к электронному почтовому ящику из разных мест и с различных систем. К примеру, пользователь может проверять свой почтовый ящик с настольного компьютера в офисе, с домашнего ПК и с мобильного компьютера в дороге.

Из такой ситуации существует два выхода. Первый – оставлять копии сообщений на сервере. В таком случае сообщения будут сохраняться на сервере, пока не будет достигнут максимально допустимый объем почтового ящика, устанавливаемый провайдером. Тогда почта перестанет приниматься ящиком. Другой подход состоит в интерактивном способе работы с почтовым ящиком, обеспечиваемом протоколом IMAP. Абонент вводит имя и пароль и получает доступ к своей корреспонденции, не загружая ее на свой компьютер, а просматривая непосредственно на сервере. Недостаток подхода в том, что для него требуется постоянное соединение с интернетом.

Протоколы гипертекстовой передачи данных

HTTP[83] является одним из протоколов WWW, включающей в себя еще несколько средств работы с документами: HTML[84], CGI[85] и URL. Основное назначение HTTP – извлечение HTML-документов, адресуемых с помощью URL. WWW-клиент посылает запросы серверу и получает документы в качестве ответа.

HTTP основывается на парадигме запросов/ответов. Запрашивающая программа-клиент устанавливает связь с обслуживающей программой-сервером и посылает запрос серверу в форме, содержащей служебную информацию и тело сообщения:

- метод запроса;
- URL;

[83] HTTP – Hypertext transition protocol.
[84] Hypertext markup language – язык гипертекстовой разметки.
[85] CGI – Common gateway interface, общий шлюзовый интерфейс

- версия протокола
- управляющая информация запроса;
- информация о клиенте;
- тело сообщения (если необходимо).

Таким образом, в служебной части запроса указывается метод и объект, к которому этот метод применяется. Объект идентифицируется при помощи URL.

Сервер отвечает сообщением, содержащим следующие части:

- строка статуса (включая версию протокола и код состояния – успех или ошибка);
- информация о сервере (программное обеспечение, его версия, значения некоторых системных переменных);
- метаинформация о содержании ответа;
- тело ответа (если есть).

Существует 5 категорий результатов или кодов состояния. Первая цифра кода состояния определяет класс ответа:

- *1xx: информационные коды* – запрос получен, продолжается обработка;
- *2xx: успешные коды* – действие было успешно получено, понято и обработано;
- *3xx: коды перенаправления* – для выполнения запроса должны быть предприняты дальнейшие действия;
- *4xx: коды ошибок клиента* – запрос имеет некорректный синтаксис или не может быть выполнен по какой-то другой причине, зависящей от клиента;
- *5xx: коды ошибок сервера* – сервер не в состоянии выполнить допустимый запрос.

В табл. 11 приведен полный список кодов состояния HTTP.

Каждый раз, когда клиент желает послать запрос серверу, он должен открыть соединение, которое закрывается сервером после посылки ответа. Таким образом, сервер не имеет информации о результатах выполнения предыдущих запросов.

Следует отметить, что одна программа может быть одновременно и клиентом и сервером. Использование этих терминов в данном тексте относится только к роли, выполняемой программой в течение данного конкретного сеанса связи, а не к общим функциям программы.

Таблица 11. Коды состояния HTTP

1xx	**Информационные коды.**	
100	**Continue**	Клиент может продолжать запрос.
101	**Switching Protocols**	Сервер принял запрос клиента на переключение на модифицированный протокол.
2xx	**Успешные коды**	
200	**Ok**	Успешный запрос.
201	**Created**	Запрос выполнен, в результате этого был создан новый запрос.
202	**Accepted**	Запрос был принят на обработку, но обработка не завершена.
203	**Non-Authoritative Information**	Возвращенная информация была собрана с копии третьей стороны.
204	**No Content**	Сервер обработал запрос, но в результате данные не получены.
205	**Reset Content**	Пользовательский агент переустановит отображение документа.
206	**Partial Content**	Сервер выполнил частичный запрос GET к документу.
3xx	**Коды перенаправления**	
300	**Multiple Choices**	Этот заголовок используется для того, чтобы показать, что удовлетворять запрос может более чем один документ.
301	**Moved Permanently**	Запрошенный документ был перенесен на новый URI.
302	**Found**	Запрошенный ресурс был временно перемещен на новый URI.
303	**See Other**	Ответ на запрос можно найти под различными URI. Он может быть выбран с помощью запроса, сделанного методом GET к этому ресурсу.
304	**Not Modified**	Сервер отвечает этим кодом, когда клиент выполнил условный запрос GET и запрос был разрешен, но документ не модифицирован.
305	**Use Proxy**	Доступ к запрошенному ресурсу должен производиться через proxy, заданный в поле Location . Поле Location задает URI для proxy.
307	**Temporary Redirect**	Запрошенный ресурс временно находится под другими URI. Так как переадресация может быть отменена в любой удобный момент, для будущих запросов клиент должен использовать Request-URI.
4xx	**Коды ошибок клиента**	
400	**Bad Request**	Запрос не понят сервером из-за наличия синтаксической ошибки.
401	**Unauthorized**	Запрос требует идентификации пользователя.
402	**Payment Required**	Требуется оплата.
403	**Forbidden**	Сервер понял запрос, но он отказывается его выполнять. Запрещено. Идентификация тут не помогает.
404	**Not Found**	Сервер не нашел соответствия по запросу Request-URI.
405	**Method Not Allowed**	Метод, указанный в Request-Line, не соответствует ресурсу, заданному Request-URI.

406	**Not Acceptable**	Ресурс, определенный запросом, может генерировать только ответ, характеристики которого не соответствуют заголовкам, посланным в запросе.
407	**Proxy Authentication Required**	Этот код подобен коду 401 (unauthorized), но в этом случае клиент должен сначала идентифицировать себя с помощью proxy.
408	**Request Time-out**	На протяжении периода ожидания сервера клиент не сделал запроса.
409	**Conflict**	Запрос не будет завершен вследствие конфликта с текущим состоянием ресурса.
410	**Gone**	Запрошенный ресурс и адрес, по которому можно сделать пересылку, на сервере отсутствуют.
411	**Length Required**	Сервер отказывается принимать запрос без определенного Content-Length.
412	**Precondition Failed**	При проверке на сервере одного или более полей заголовка запроса обнаружено несоответствие.
413	**Request Entity Too Large**	Сервер отказывается обрабатывать запрос потому, что размер запроса больше того, что может обработать сервер.
414	**Request-URI Too Large**	Сервер отказывается обрабатывать запрос потому, что Request-URI превышает размеры, которые может обработать сервер.
415	**Unsupported Media Type**	Неподдерживаемый медиа тип.
5xx	**Коды ошибок сервера**	
500	**Internal Server Error**	Внутренняя ошибка сервера.
501	**Not Implemented**	Сервер не поддерживает возможностей, необходимых для обработки запроса.
502	**Bad Gateway**	Сервер, функционирующий как шлюз или proxy, получил ошибочный ответ от подчиненного сервера, к которому он попытался получить доступ для обработки запроса.
503	**Service Unavailable**	В данный момент сервер не в состоянии обработать запрос из-за того, что сервер перегружен или находится на профилактическом обслуживании.
504	**Gateway Time-out**	Работая в режиме шлюза или proxy[86], сервер не получил вовремя ответ от сервера верхнего уровня.
505	**HTTP Version not supported**	Сервер не поддерживает или отказывается поддерживать версию протокола HTTP, которая была использована в последнем запросе.

[86] Прокси-сервер (от англ. proxy – «представитель, уполномоченный») – служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственной буферной памяти. В некоторых случаях запрос клиента или ответ сервера может быть изменен прокси-сервером в определенных целях.

Базовая структура WWW основана на том, что протокол HTTP работает как обобщенное средство передачи различных типов информации от сервера к клиенту. Каждая сущность, которая может быть предоставлена, идентифицируется уникальным образом с помощью URL.

Указатели ресурсов

Одной из целей проекта WWW была разработка стандартного способа указания ссылок на доступные в интернете ресурсы, применимого для любых типов ресурсов (документы, звуковые файлы и т. д.). Для решения этой задачи было введено понятие URL[87].

URL представляет собой описание местонахождения ресурса в интернете. При этом рассматриваемый ресурс может представлять собой как файл на локальном диске компьютера, так и файл, находящийся на каком-либо сервере интернета в любой части света.

URL может быть представлен в виде абсолютной или относительной ссылки. Абсолютная ссылка содержит полную информацию о ресурсе, включая имя компьютера, на котором он находится, путь к соответствующему каталогу и имя файла. При использовании относительных ссылок предполагается, что хост-компьютер и путь к текущему каталогу уже были определены в ходе предшествующей работы, поэтому указывается только имя файла (или путь с подкаталогами и имя файла).

Структура URL-адреса показана на рис. 25.

Программы просмотра (браузеры)

Для работы с системой WWW по протоколу HTTP необходимо использовать специальную программу просмотра, называемую WWW-браузер или просто браузер[88]. Браузер — это прикладная программа, взаимодействующая с WWW, получающая затребованные документы, интерпретирующая данные и отображающая содержание документов на экране. WWW-документы представляют собой гипертекст. В отличие от обычных текстов, WWW-документы содержат команды, задающие структуру документа (заголовки

[87] URL – Uniform resource locator, универсальный указатель ресурса.

[88] Браузер – от англ. *browse* – просматривать, программа-клиент, предоставляющая пользователю возможности навигации и просмотра веб-ресурсов, скачивания файлов и т.п. Часто в комплекте с браузерами поставляются почтовые программы, средства работы с серверами новостей и средства общения в реальном времени.

разных уровней, абзацы основного текста и т. д.), что дает возможность браузеру отформатировать документ при его отображении на экране в соответствии с возможностями конкретного компьютера, а также URL-ссылки на другие текстовые документы. Это дает возможность при чтении некоторого текста легко и быстро переходить к другой, связанной с ним по смыслу текстовой информации. Такой связанный посредством ссылки текст может представлять собой как фрагмент текста того же документа, так и другой текстовый или бинарный документ.

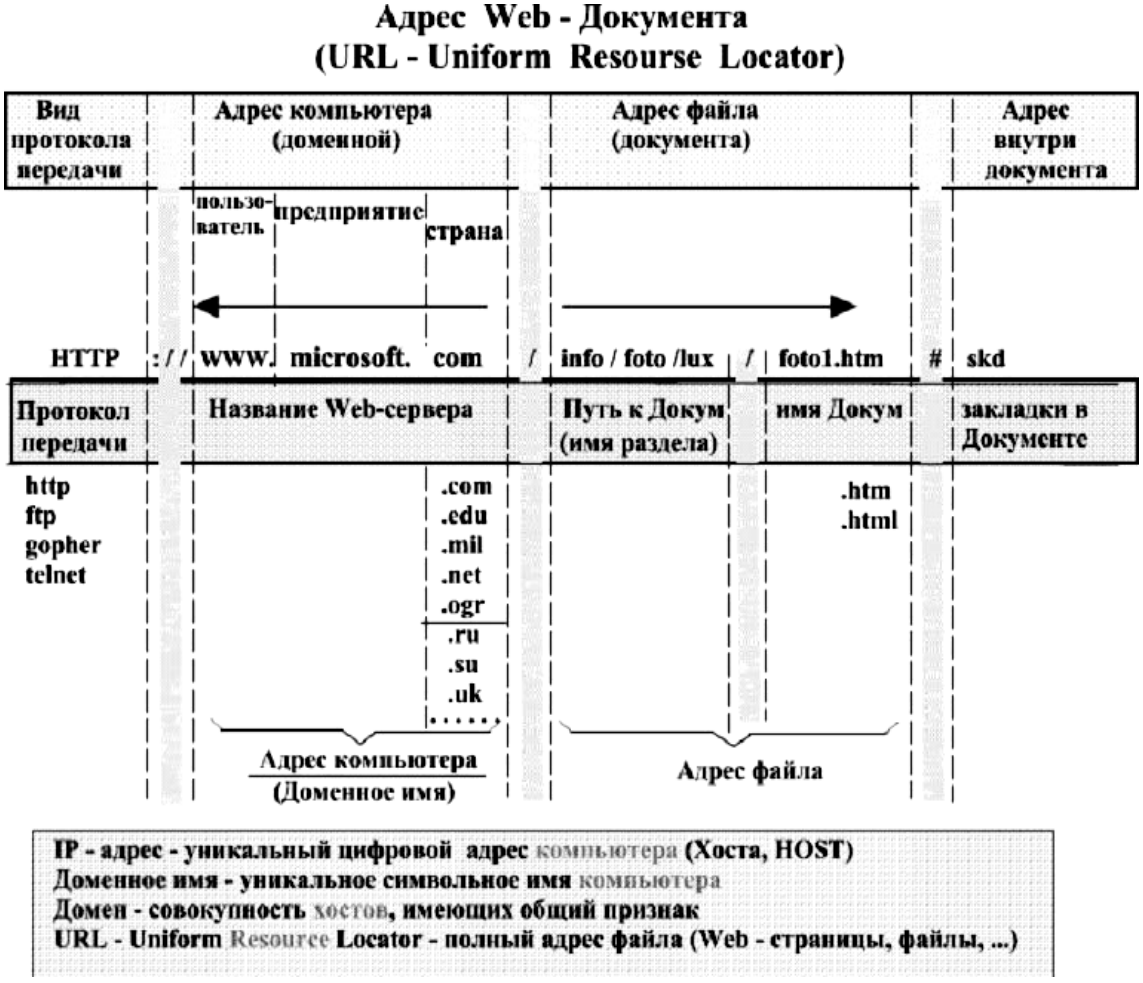


Рис. 25. Структура URL-адреса.

Для создания гипертекстовых документов используются специализированные языки, носящие общее название *языков разметки*. Наиболее распространенным из них является язык HTML, представляющий собой достаточно простой набор команд, которые описывают структуру документа. Этот язык разметки позволяет выделить в документе отдельные логические фрагменты (заголовки, абзацы, списки-перечисления и т.д.), и задать некоторые простейшие атрибуты форматирования. Браузер получает документ, интер-

претирует HTML-команды и выполняет форматирование составных частей документа (заголовков, перечислений, абзацев, таблиц и т. д.) так, чтобы обеспечить наиболее удачное расположение информации на дисплее.

Обзорная информация по языкам разметки приведена в приложении 4.

Примеры браузеров: NCSA Mosaic[89], Netscape Navigator, Microsoft Internet Explorer, Opera, Mozilla, Arachne, Lynx, Links, Konqueror, Galeon и др.

Контрольные вопросы к разделу

1. Что такое «распределенная вычислительная система»? Какие категории таких систем вы можете назвать и в чем их принципиальные различия. Приведите примеры.
2. Что представляет собой эталонная модель ISO OSI? За что отвечает каждый уровень модели? Какие недостатки модели вы можете назвать? Приведите примеры протоколов, соответствующих уровням.
3. Что такое протокол, интерфейс и сервис? Какие функции выполняет каждый из них? Что такое стек протоколов?
4. Что представляет собой модель TCP/IP? За что отвечают уровни модели и как они соответствуют эталонной модели OSI? Какие протоколы применяются на уровнях? Какие недостатки и достоинства модели можно назвать? В чем принципиальные отличия этих двух моделей?
5. Опишите стандартные стеки коммуникационных протоколов. Приведите конкретные примеры протоколов, функционирующих в рамках этих стеков.
6. Перечислите стандарты IEEE 802. Для чего нужна стандартизация сетевых технологий? Как вы думаете, какие технологии получат развитие в следующих подстандартах 802?
7. Что представляет собой сетевая технология Ethernet? Что такое «принцип случайного доступа»? Как вы думаете, на каком еще принципе можно основывать доступ к сетевой среде передачи данных?
8. Какие методы коммутации вы можете назвать? Опишите их достоинства и недостатки. Какие из этих методов используются наиболее широко, а какие уже практически вышли из употребления?
9. Что такое мультиплексирование и для чего оно служит? Назовите способы мультиплексирования. Чем они отличаются, каковы достоинства и недостатки каждого метода?
10. Какие проблемы построения вычислительных сетей вы можете назвать? Опишите способы решения или обхода этих проблем.

[89] Первый браузер был разработан студентами факультета NCSA (National center for supercomputing applications, Национальный центр суперкомпьютерных приложений) из университета в Иллинойсе и назывался Mosaic. Развитие браузера продолжалось до 1997 года.

11. В чем принципиальные особенности сетей, основанных на технологии X.25? Опишите модель сети X.25. Какие достоинства и недостатки вы можете назвать? Где применяются такие сети?
12. Что представляют собой сети frame relay? На какой модели они основаны, в чем их достоинства и недостатки?
13. Какая область является наиболее привлекательной для построения сетей по технологии ATM? А какая – наиболее реальной? В чем особенности таких сетей, их достоинства и недостатки? Опишите сетевую модель ATM, в чем она согласуется с моделью OSI, а в чем – нет?
14. Приведите примеры топологии вычислительных сетей. Какие достоинства и недостатки вы можете назвать для каждой из них? Чем отличается физическая топология от логической, и какие преимущества дает каждая из таких структуризаций?
15. Что такое локализация трафика и какой она имеет смысл? Как ее достичь? Объясните особенности и распространение различных типов трафика 10 лет назад, 5 лет назад, сегодня и (предположительно) через 5 лет.
16. Какие коммуникационные устройства вы можете назвать? В чем их особенности? Для чего служит каждое из них?
17. Опишите технологии организации беспроводной вычислительной сети. Каковы достоинства и недостатки таких сетей, ограничения и область применения? Какие вы видите перспективы развития технологий беспроводной передачи данных?
18. Какие вы знаете способы адресации устройств в вычислительных сетях? Каким образом назначаются адреса компьютерам и устройствам, как они выглядят? Раскройте структуру IP-адреса по стандартам IPv4 и IPv6.
19. Перечислите требования, предъявляемые к компьютерным сетям. Чем обусловлены эти требования? Каким образом обеспечивается их выполнение? Как соблюсти баланс между взаимопротиворечащими требованиями и на чем основывается понятие «качество обслуживания»?
20. По каким признакам классифицируют вычислительные сети? Какие достоинства и недостатки этих способов классификации вы можете назвать? Предложите свой способ классификации вычислительных сетей.
21. Опишите основные принципы функционирования интернета.
22. Раскройте понятие «доменная система имен». Что обусловило появление этого сервиса, каковы основные этапы его развития? Каково состояние DNS в настоящее время?
23. Что представляет собой протокол гипертекстовой передачи данных? Что такое «ошибка 404», и как избежать ее и других ошибок при запросе к ресурсам в интернете?

2. ОБЗОР ГЛОБАЛЬНЫХ ИНФОРМАЦИОННЫХ СЕТЕЙ

2.1. ARPANET (Интернет, часть 1)

Первым документальным описанием социального взаимодействия, которое станет возможным благодаря глобальной сети, была серия заметок, написанных Дж. Ликлайдером из Массачусетского технологического института (MIT) в августе 1962 года. В этих заметках обсуждалась концепция «галактической сети». Автор предвидел создание глобальной сети взаимосвязанных компьютеров, с помощью которой каждый сможет быстро получать доступ к данным и программам, расположенным на любом компьютере. По духу эта фантастическая в то время идея очень близка к современному состоянию интернета. В октябре 1962 года Ликлайдер стал первым руководителем исследовательского компьютерного проекта в ARPA[90] и сумел убедить руководство и своих сотрудников в важности этой сетевой концепции.

Первая статья по теории пакетной коммутации была опубликована в июле 1961 года, а первая книга – в 1964 году. Теоретическая обоснованность пакетных коммутаций явилась важным шагом на пути создания компьютерных сетей. Другим ключевым шагом стала организация реального межкомпьютерного взаимодействия. В 1965 году компьютер TX-2, расположенный в Массачусетсе, был связан с ЭВМ Q-32, находившейся в Калифорнии. Связь осуществлялась по низкоскоростной коммутируемой телефонной линии. Таким образом была создана первая в истории (хотя и маленькая) нелокальная компьютерная сеть. Результатом эксперимента стало понимание того, что компьютеры с разделением времени могут успешно работать вместе, выполняя программы и осуществляя выборку данных на удаленной машине. Стало ясно и то, что телефонная система с коммутацией соединений абсолютно непригодна для построения компьютерной сети. Перспективы виделись в развитии пакетной коммутации.

В 1960-е годы, после Карибского кризиса, фирма RAND[91], один из моз-

---

[90] ARPA (The Advanced research projects agency, Управление перспективных исследовательских программ) – американское федеральное агентство, подчиненное Министерству обороны США, создано в 1957 г. В 1972 г. в связи с переходом под юрисдикцию Пентагона было переименовано в DARPA (The Defense advanced research projects agency), а в 1990 г. снова вернулось к первоначальному названию ARPA.

[91] RAND Corporation – американская некоммерческая организация, занимавшаяся стратегическими исследованиями и разработками.

говых центров Соединенных Штатов Америки, предложила создать децентрализованную компьютерную сеть. Проект включал в себя объединение компьютеров военных, научных и образовательных учреждений в компьютерную сеть, которая смогла бы сохранить свою работоспособность в условиях ядерной атаки. Основной идеей проекта была децентрализация управления и подчинения, чтобы выход из строя одного или нескольких сегментов сети не привел к ее коллапсу. Такая структура могла быть осуществлена только при наличии между узлами сети множественных каналов связи. В первом варианте предложения (1964 г.) просто утверждалось, что все узлы сети должны иметь одинаковый статус. Любой узел должен быть уполномочен порождать, передавать и получать сообщения от любого другого. Сообщения разбиваются на небольшие стандартизованные элементы, называемые пакетами. В пакете указывается поле места назначения, и доставка обеспечивается тем, что каждый узел уполномочен посылать(или переадресовывать) пакеты по сети к месту назначения.

В 1967 году DARPA опубликовала концепцию и план ARPANET. Интересно, что на конференции, где представлялся доклад об осуществленных разработках, был сделан еще один доклад о концепции пакетной сети. Выяснилось, что практически одновременно работы в области пакетной коммутации велись в MIT (1961-1967), RAND (1962-1965) и NPL[92] (1964-1967) при полном отсутствии информации о деятельности друг друга.

В конце 1960-х годов эксперименты с концепцией децентрализованной сети начались проводиться корпорацией RAND совместно с Массачусетским технологическим институтом и Калифорнийским университетом Лос-Анджелеса. Также эксперименты проводились в Великобритании. В 1968 году ARPA открыло финансирование этого проекта в США. Работы велись совместно ARPA и фирмой BBN[93], между которыми был заключен контракт на создание программного обеспечения. К сентябрю 1969 года появилась на свет ARPANET – первая в мире децентрализованная сеть. В основу проекта были положены три основные идеи:

---

[92] National physic laboratory – Британская Национальная физическая лаборатория.

[93] BBN – Bolt, Beranek and Newman, первоначально консалтинговая фирма, позднее корпорация. Фирму основали в 1951 году Ричард Болт, глава акустической лаборатории Массачусетского института технологий; Лео Беранек, технический директор акустической лаборатории; и Роберт Ньюман, студент Ричарда Болта. В послужном списке фирмы – первый сетевой маршрутизатор, первое электронное письмо, протокол TCP и многое другое.

- каждый узел сети соединен с другими, так что существует несколько различных путей от узла к узлу.
- все узлы и связи рассматриваются как ненадежные
- существуют автоматически обновляемые таблицы перенаправления пакетов (маршрутизации) – пакет, предназначенный для несоседнего узла, отправляется на ближайший к нему, согласно таблице перенаправления пакетов, при недоступности этого узла – на следующий и т.д.Первая версия ARPANET состояла из четырех узлов:
- компьютер SDS SIGMA 7 в Калифорнийском университете Лос-Анджелеса;
- компьютер SDS940 в Стэндфордском исследовательском институте[94];
- компьютер IBM360 в Калифорнийском университете Санта-Барбары;
- компьютер DEC PDP-10 в Университете штата Юта.

Соединение этих компьютеров между собой было осуществлено 29 октября 1969 года. Эта дата считается днем рождения Интернета. Испытания ARPANET оказались крайне успешными. Ученые исследовательских учреждений получили возможность обмениваться данными об проведенных исследованиях. Уже в 1971 году ARPANET включала в себя Массачусетский технологический институт, RAND, Гарвард, Питтсбургский университет Карнеги–Меллона, Case western reserve, центр NASA в Эймсе. К 1972 году сеть ARPANET насчитывала 37 узлов, а в 1973 году к сети были впервые подключены зарубежные узлы – Университетский колледж в Лондоне и Королевская лаборатория радиолокации в Норвегии. Необходимо отметить, что, несмотря на то, что изначально ARPANET связывала самые престижные исследова-

[94] Этот компьютер интересен еще и тем, что находился в лаборатории Дугласа Энгельбарта и использовался в работах над амбициозной концепцией под условным названием «Расширение человеческого интеллекта». Из этого проекта, в частности, вышли такие разработки, как компьютерная мышь и графический интерфейс пользователя.

Дуглас Карл Энгельбарт, род. 30 января 1925, – один из первых исследователей человеко-машинного интерфейса. Энгельбарт создал: первую систему обмена текстовыми сообщениями; протоколы для виртуальных терминалов; множественные окна (открытие нового сегмента данных для прикладной программы при запуске); протокол удаленного доступа, ссылки, работал в области гипермедиа. Стремился к совершенствованию интеллектуальных способностей человека, создал общественный институт, работающий в данном направлении.

Энгельбарт является автором более 25 трудов, имеет 20 патентов на изобретения (в том числе на компьютерную мышь) и множество наград.

тельские институты США, и основное назначение сети – средство удаленного доступа к компьютерам, значительная часть потока информации со временем наполнилась личными сообщениями, сплетнями и просто пустой болтовней. В целом же концепция децентрализованной сети с пакетной передачей данных и сама ARPANET означали огромный успех.

В октябре 1972 года была организована большая, весьма успешная демонстрация ARPANET на Международной конференции по компьютерным коммуникациям. Это был первый показ новой сетевой технологии на публике. В том же 1972 году появилось первое широко востребованное приложение – электронная почта. В марте Рэй Томлинсон из BBN, движимый необходимостью создания для разработчиков ARPANET простых средств координации, написал базовые программы пересылки и чтения электронных сообщений. Позже были добавлены возможности выдачи списка сообщений, выборочного чтения, сохранения в файле, пересылки и подготовки ответа. Таким образом, более чем на десять лет электронная почта стала крупнейшим сетевым приложением. Она не потеряла своей важности до сих пор, но для своего времени электронная почта была тем же, чем в наши дни является «всемирная паутина», – исключительно мощным катализатором роста всех видов межперсональных потоков данных.

ARPANET служила испытательным полигоном для большинства разработок в области технологий коммутации пакетов. Помимо использования ее для сетевых исследований, исследователи из нескольких университетов, военных баз, и правительственных лабораторий регулярно использовали ARPANET для обмена файлами и электронной почтой и для обеспечения удаленного доступа к их компьютерам. В 1975 году управление этой сетью было передано от DARPA к Агентству военных коммуникаций США[95], которое сделало ARPANET частью DDN[96], программы, в которой группа сетей выступала как часть всемирной коммуникационной системы для Министерства обороны США.

Несмотря на явный успех, работы были еще далеко не закончены. Лишь в 1977-79 годах архитектура и протоколы ARPANET приняли форму, в которой они известны сейчас. В это время DARPA была известна как основное агентство, финансирующее исследования в области сетей с коммутацией

[95] DCA – Defense communications agency.
[96] DDN – Defense data network, военная сеть передачи несекретных данных.

пакетов, и внедрила множество новшеств в этой области в ARPANET. ARPANET использовала обычные выделенные линии точка–точка для соединения компьютеров, но DARPA также финансировала использование коммутации пакетов в радиосетях и спутниковых линиях связи. По существу, именно растущее разнообразие аппаратных сетевых технологий вынудило DARPA изучить межсетевое взаимодействие и продвинуться по направлению к разработке объединенной сети. Доступность результатов исследований, финансировавшихся DARPA, привлекло внимание нескольких исследовательских групп, особенно тех, кто уже имел опыт использования пакетной коммутации в ARPANET. DARPA собирала неформальные встречи исследователей для обмена идеями и обсуждения результатов экспериментов. С 1979 года в проект TCP/IP включилось так много исследователей, что DARPA образовало неформальный комитет для координации и управления разработкой протоколов и архитектур развивающегося объединенного интернета[97]. Этот комитет регулярно собирался до реорганизации в 1983 году в Совет по развитию интернета[98].

В 1983 был успешно и практически безболезненно осуществлен переход ARPANET на протоколы семейства TCP/IP. Одновременно с этим МО США разделило ARPANET на две связанные сети, оставив ARPANET для экспериментальных исследований и образовав MILNET[99] для военного пользования. В нормальных условиях ARPANET и MILNET могли передавать трафик друг друга. Управление ими было организовано так, что позволяло разъединить одну сеть от другой[100].

---

[97] ICCB – Internet configuration control board, комитет по конфигурации и управлению интернетом.

[98] IAB – Internet activities board, совет по развитию интернета. Был образован из руководителей тематических групп, занимавшихся определенными технологическими областями функционирования сети.

[99] MILNET – MILitary NETwork, военная сеть. Выделена из ARPANET для обеспечения надежного сетевого сервиса в военных целях, тогда как ARPANET предназначена для исследований.

[100] Самый известный случай такого разъединения произошел в ноябре 1988 года. Он был связан с вирусом (или, вернее, червем), написанным студентом Моррисом. Интернет тогда объединял 1200 сетей, включающих 85200 узловых компьютеров на территории США и Европы. В течение трех дней вирусом было инфицировано 6200 машин. Поражены вычислительные центры Корнельского (Нью-Йорк), Стэнфордского (Калифорния), Принстонского (Нью-Джерси) и ряда других университетов, вычислительные центры подсети MILNET, ряд исследовательских институтов и лабораторий, работающих на Министерство обороны США: Rand Corporation, Ливерморская лаборатория им. Лоуренса, Ис-

Так как ARPANET ежедневно использовалась исследователями, разрабатывающими архитектуру Интернета, она оказывала большое влияние на их работу. Так, они пришли к мысли использовать ARPANET как глобальную магистральную сеть, на основе которой можно создать Интернет. Влияние идеологии одной, центральной глобальной магистральной сети до сих пор ощущается в некоторых из протоколов Интернета, и привело к тому, что добавление к интернату дополнительных магистральных сетей является непростой задачей.

Физически ARPANET состояла из приблизительно 50 миникомпьютеров C30 и C300 корпорации BBN, называемых узлами коммутации пакетов (PSN[101]), разбросанных по континентальной части США и западной Европе (MILNET имеет приблизительно 160 PSN, включая 34 в Европе и 18 в Тихом Океане и на Дальнем Востоке). В каждом из мест, участвующем в работе сети, располагается один PSN, который предназначен для коммутации пакетов; он не может быть использован для других целей. На самом деле, все PSN считаются частью ARPANET и управляются Центром Сетевых Операций (NOC), размещенным в фирме BBN в Кембридже, штат Массачусетс.

Линии данных точка–точка, арендованные у фирм, предоставляющих глобальные линии связи, соединяют вместе PSN, образуя из них сеть. Например, арендованная линия связи соединяет PSN, находящийся в университете Пурдью, с PSN в Карнеги-Меллоне и с PSN в университете Висконсина. Вначале большинство из выделенных линий в ARPANET работало со скоростью 56 Кбит/с, скоростью, которая считалась очень большой в 1968 году, но оказалась медленной по современным меркам. Напомним, что скорость следует представлять как меру пропускной способности, а не время, нужное для доставки пакетов. Чем больше компьютеров использовало ARPANET, тем большей делали пропускную способность, чтобы приспособиться к этой загрузке.

Принцип дублирования применяется во всех военных системах, так как

следовательский центр НАСА, Армейская лаборатория баллистики и многие другие. Общие подсчитанные потери от вируса составили около 100 млн. долларов. К расследованию было подключено ФБР. К счастью, вирус, блокируя работу сети, не портил саму информацию. Тем не менее, по характеру последствий данный случай был расценен как национальная катастрофа. Результаты исследований действия вируса и выбора необходимых мер по ликвидации последствий были быстро засекречены, публикации, посвященные этому случаю, прекратились.

[101] PSN – Packet switch node, узел коммутации пакетов. Раньше назывались IMP – Interface message processor, интерфейсные процессоры сообщений.

важна надежность системы. При создании ARPANET агентство DARPA решило следовать военным требованиям надежности, поэтому они потребовали, чтобы каждый PSN имел по меньшей мере две выделенных линии для связи с другими PSN, и чтобы программное обеспечение автоматически адаптировалось к сбоям и выбирало другие пути. В результате ARPANET продолжает работать, даже если один из каналов вышел из строя.

Помимо соединения с выделенными линиями, каждый PSN ARPANET имеет до 22 портов, соединяющих его с хостами компьютерами пользователей. Первоначально все компьютеры, которым требовался доступ к ARPANET, присоединялись напрямую к одному из портов PSN. Обычно прямые соединения осуществлялись с помощью специальной интерфейсной платы, которую соединяли с шиной ввода-вывода компьютера и присоединяли к порту хоста в PSN. При правильном программировании этот интерфейс позволял компьютеру контактировать с PSN для посылки и приема пакетов.

Старое оборудование порта PSN использовало сложный протокол для передачи данных по ARPANET. Этот протокол называется 1822[102] и по-прежнему используется в портах PSN в MILNET. В общем, 1822 позволяет хосту послать пакет по ARPANET к указанному PSN и к указанному порту этого PSN. Процесс передачи является довольно сложным, так как 1822 предоставляет надежную доставку с управлением потоком. Чтобы предотвратить перегрузку сети каким-либо хостом, 1822 ограничивает число одновременно передаваемых пакетов. Чтобы гарантировать, что каждый пакет достигает получателя, 1822 заставляет отправителя ждать сигнала RFNM[103] от PSN перед передачей каждого пакета. RFNM выступает здесь в качестве подтверждения. Он включает схему резервирования буферов, которая требует от отправителя резервирования буфера в PSN получателя перед посылкой пакета.

По существу, ARPANET – это просто механизм передачи. Когда компьютер, присоединенный к одному порту, посылает пакет другому порту, доставляются только те данные, которые были переданы. Так как ARPANET не доставляет сетевого заголовка, пакет, передаваемый по ней, не имеет специального поля для указания типа пакета. Поэтому, в отличие от других сетевых технологий, ARPANET не доставляет самоидентифицирующиеся пакеты. В результате получается, что ARPANET не понимает содержимое па-

[102] По номеру технического отчета, в котором он был опубликован.
[103] RFNM – Request for next message, готов к следующему сообщению.

кетов, которые передаются по ней; согласование форматов и содержимого пакетов происходит между машинами, присоединенными к ARPANET, при их передаче или получении на конкретных портах PSN.

Протокол 1822 не стал промышленным стандартом. Так как лишь несколько производителей делали интерфейсные платы для 1822, стало трудно присоединять новые машины к ARPANET. Для решения этой проблемы DARPA разработало новый интерфейс PSN, который использует международный стандарт передачи данных, известный как X.25[104]. Первая версия реализации PSN с X.25 использовала только часть передачи данных стандарта X.25 (известную как HDLC/LAPB[105]), но более поздние версии использовали весь X.25 при соединении с PSN (в результате ARPANET стал выглядеть как сеть X.25). Многие порты MILNET теперь используют X.25.

Внутри, естественно, ARPANET использовала собственный набор протоколов, которые невидимы пользователям. Например, существовал один специальный протокол, который позволял PSN запрашивать состояние других PSN; другой протокол, который PSN использовали для посылки пакетов между собой; и еще один протокол, позволявший PSN обмениваться информацией о состоянии каналов и оптимальных маршрутах.

Так как ARPANET изначально был создан как автономная, независимая сеть, используемая для исследований, ее протоколы и структура адресов были разработаны без учета возможных расширений. В середине 1970-х годов стало ясно, что одна сеть не в состоянии решить все коммуникационные проблемы, и DARPA начало исследовать сетевые технологии, использующие спутники и пакетные радиосети. Опыт, полученный при работе со всеми этими сетевыми технологиями, лег в основу концепции межсетевого обмена.

---

[104] X.25 – сети пакетной коммутации, доступ к которым производится в соответствии с рекомендациями Международного консультативного комитета по телефонии и телеграфии (русская аббревиатура – МККТТ, английская – CCITT, Consultative committee for international telephony & telegraphy; современное название этого комитета – Международный союз электросвязи или ITU-T, International telecommunications union-telecommunications standardization sector) – «X.25». Первый вариант Рекомендации X.25 МККТТ был выпущен в 1976 году.

[105] HDLC – High level data link control, высший уровень управления каналом данных. Стандарт канального уровня для связей «точка-точка» и многоточечной. LAPB – Link access procedure balanced; Link access protocol balanced, сбалансированный протокол (или процедура) доступа к каналу. Протокол, используемый для доступа в сети X.25 на канальном уровне, относится к числу полнодуплексных протоколов «точка-точка» с битовой синхронизацией.

ARPANET была расформирована в июне 1990. MILNET продолжает оставаться магистральной сетью военной части объединенного Интернета. Центр управления MILNET, находящийся возле Вашингтона, следит за трафиком 24 часа в сутки, обнаруживает поломки в оборудовании и линиях связи и координирует установку нового программного обеспечения на PSN. ARPA принимает участие в FNC[106] для финансирования разработок и экспериментов, которые помогают в создании NREN[107].

2.2. SPRINT

Sprint network – глобальная информационная сеть, созданная корпорацией Sprint International, которая до сих пор осуществляет управление сетью и ее развитие. Сеть Sprint обеспечивает взаимодействие абонентских систем, в том числе и телефонных аппаратов в более чем 160 странах. Коммуникационная сеть покрывает все континенты и содержит более 100 узлов коммутации, а сервис, связанный с проведением видеоконференций, охватывает десятки стран.

Сеть имеет более 50 международных узлов коммутации и взаимодействует более чем с 3000 национальными и фирменными сетями. В сети широко используются оптические каналы. Основные абонентские интерфейсы сети определяются рекомендациями X.25, X.32[108].

Sprint предоставляет пользователям ряд глобальных сетевых служб. К ним относятся:

- электронная почта, передающая сообщения и обеспечивающая работу телексов;
- служба факсимильной связи, осуществляющая доставку документов в любую точку земли;
- сервис, связанный с проведением расчетов на основе магнитных кар-

[106] FNC – Federal networking council, федеральный совет по сетям. Организация, ответственная за удовлетворение сетевых потребностей федеральных агентств США.

[107] NREN – National research and education network, национальная сеть исследований и обучения. Образована в 1991 году и первоначально связала суперкомпьютерные центры США, сделав их доступными ученым, преподавателям и студентам небольших колледжей и университетов. В настоящее время многие государства поддерживают существование сетей, аналогичных NREN. Например, в Татарстане это SENet – Science and education network, Научная образовательная сеть, образована в 2000 году и объединяет институты Казанского научного центра РАН, Академии наук Республики Татарстан, высшие учебные заведения города Казани.

[108] X.32 – интерфейсы сети коммутации пакетов.

точек и компьютерных карточек;

- крупная коммуникационная сеть, передающая любые типы данных, поддерживая работу других служб.

В сети также функционируют банковские системы, обеспечиваются межбанковские платежи. Существуют закрытые банковские виртуальные сети, создаваемые для групп банков. Для увеличения пропускной способности в Sprint широко используется асинхронный способ передачи. Это обеспечивает функционирование сетевых служб в режиме реального времени.

2.3. SWIFT

SWIFT[109] network – банковская сеть региональных центров, предназначенная для выполнения межбанковских расчетов. SWIFT является глобальной сетью, и ее компоненты расположены во всех частях света. Сеть широко использует технологию открытых систем. Для этого введено новое семейство интерфейсов Alliance, что позволяет внедрять однотипные прикладные процессы в различные национальные и частные сети, связанные со SWIFT. Интерфейсы также обеспечивают доступ к базам данных через сети телекса и факсимильной связи.

Для SWIFT разработаны стандарты документов, пересылаемых банками. Идентификация последних осуществляется с помощью кодов BIC[110]. Каждый код определяет 11-битовый адрес банка. SWIFT состоит из абонентских систем банков, каналов, концентраторов и операционных центров. Эти центры управляют работой сети.

Новая реализация сети, SWIFT II, построена на основе архитектуры, разделяющей сеть на следующие четыре слоя:

- *терминалы пользователей*, которые должны пройти сертификацию;
- *региональные процессоры*, производящие предварительную проверку сообщений пользователей;
- *групповые процессоры*, обеспечивающие хранение сообщений и их

[109] SWIFT – Society for worldwide interbank financial telecommunications, объединение международной межбанковской финансовой связи. Создано в мае 1973 г. при участии 513 банков из 15 стран. С него началось создание межбанковских систем. Штаб-квартира SWIFT находится в Бельгии. Объединение существует за счет вступительных взносов и ежегодных платежей членов-акционеров.

[110] BIC – Banking identifier code, код идентификации банка.

распределение по региональным процессорам;

• *системные управляющие процессоры*, выполняющие функции контроля и управления сетью.

Особые меры принимаются по обеспечению безопасности данных. Сеть распознает каждый терминал по его секретному коду и анализу присланного сообщения. Каждое сообщение получает свой номер, который отслеживается в сети. Обеспечивается шифрование текста сообщения. Пользователям направляются отчеты об обмене сообщениями.

SWIFT объединяет свыше 6500 банковских систем, расположенных почти в ста странах. Ее задачей является обеспечение международных финансовых расчетов между юридическими и физическими лицами. Включение в сеть SWIFT требует, как правило, серьезной реорганизации и автоматизации работы банков. Поэтому вновь подключаемые к сети банки проходят «кандидатский» стаж в течение 52 недель и начинают работать с 1 января очередного года. При этом «кандидат» должен внести солидную сумму взноса и купить хотя бы одну акцию общества SWIFT. Сеть обеспечивает перевод денежных средств за 20 минут при обычном приоритете и за 5 минут – при срочном приоритете.

Сообщение в сети готовится в формате SWIFT. Адрес банка включает четырехзначный код банка, двухразрядный код страны по стандарту ISO и двухразрядный код места нахождения. В сети принимаются строгие меры безопасности данных. Они также касаются методов вхождения абонентов в сеть, распознавания сообщений по исходящим и входящим номерам, шифровка этих сообщений с помощью специальных средств. В сети устанавливается программное обеспечение, специально разработанное для SWIFT. Сеть выполняет не только межбанковские операции, но и операции с ценными бумагами.

2.4. TRANSPAC

Transpac network – международная коммуникационная сеть, созданная министерством связи Франции в 1978 г. Основным интерфейсом абонента являются X.25 и X.32. Сеть содержит узлы коммутации пакетов и магистральные каналы. Сеть работает с коэффициентом ошибок 1/1000 млрд. бит, коэффициентом неготовности 3/10000. Transpac обеспечивает многие виды сервиса: диалоговые соединения, сбор данных с отсроченной передачей, передача пакетов, электронная почта, видеотекс и т.д.

2.5. BITNET

BITNET была создана для стимулирования творческой деятельности в университетах. Она была создана в 1981 г. корпорацией IBM с целью способствовать общению преподавателей и сотрудников американских университетов и других подобных организаций, к 1988 году насчитывала более 2200 хост-машин. Принцип, на котором построена сеть, прост. Каждое учебное заведение само платит за связь с BITNET и обязуется подключить через свой канал к сети хотя бы одну новую организацию. По мере роста сети каждый ее участник соглашается бесплатно пересылать информацию другим. Компьютеры BITNET используют метод передачи с промежуточным хранением. Это значит, что файл передается от одного узла к другому через ряд промежуточных точек. Прежде чем цепочка будет продолжена, каждый файл должен быть целиком передан с данного узла на следующий. Если соединение между двумя компьютерами прерывается, файл просто сохраняется на текущем узле до тех пор, пока канал передачи не будет восстановлен. Информация к каждому узлу может попасть по одному-единственному маршруту, со всеми вытекающими ограничениями.

В целом система работала, но из-за особенностей потока данных в сети такой топологии возникли проблемы: медленная скорость передачи и отсутствие запаса пропускной способности. Решение заключалось в переносе трафика BITNET на использование протоколов интернета, что обеспечивало возможность альтернативной маршрутизации и более высокие скорости передачи, присутствующие в средах TCP/IP. В 1989 г. сеть BITNET подверглась реорганизации и получила имя BITNET II. В каждом из регионов был создан собственный главный узел. В свою очередь эти узлы были связаны высокоскоростными линиями передачи данных, и в результате возникла высокоскоростная опорная сеть для передачи трафика BITNET.

Само слово BITNET расшифровывается как «Because it's time network», что значит: «Сеть, время которой пришло». Рост сети быстро оправдал ее название. Через 18 месяцев после создания в BITNET входило 20 университетов, в 1984 г. сеть насчитывала 100 организаций, в 1989 г. – около 500. Корпоративное название BITNET поменялось на CREN, а в 1989 г. эта сеть слилась с CSNET (Computer Science Network). CSNET прекратила существование в 1991 г.

2.6. EUnet

Сеть EUnet – одна из наиболее крупных европейских компьютерных сетей, действующая с 1982 года. EUnet имеет региональные части практически во всех европейских странах, включая страны Прибалтики, а также очень крупный российский фрагмент – сеть Relcom. EUnet объединяет около пяти тысяч хост-машин и отдельных сетей. Для пользователей российской сети Relcom важными свойствами EUnet являются:

- мощные шлюзы, соединяющие EUnet с интернетом и NSFnet;
- наличие высокоскоростной выделенной линии связи (128 Кбит/сек), соединяющей сетевой операционный центр (Амстердам, Голландия) с сетями UUNET и NSFNET в США;
- развитые прикладные службы EUnet: электронная почта, списки рассылки, архивная служба.

2.7. FIDONET

Начало сети Fidonet (или FIDO[111]) было положено в 1984 году американцами Томом Дженнингсом и Джоном Мэдиллом, которые занимались совместным написанием программного обеспечения BBS[112] под названием Fido. Проживали они на разных концах континента, в разных часовых поясах и, видимо, это натолкнуло их на мысль добавить в систему модуль, обеспечивающий организацию автоматической передачи данных по телефонной линии без вмешательства человека.

Вначале сеть состояла всего из двух *узлов* и была разработана из чистого интереса ее авторов. Однако она быстро показала свою полезность, и обмен сообщениями Fidonet вместо звонков на BBS или дорогостоящих междугородных переговоров голосом вскоре стал в порядке вещей.

---

[111] Согласно легенде, Fido – это кличка собаки основателя сети Тома Дженнингса. Также утверждают, что на самом деле никакой собаки у него нет и не было, а Фидо – это такая же распространенная в США кличка собаки, как в России, например, Шарик, Бобик или Тузик.

[112] BBS – Bulletin broadcasting service или Bulletin board system, электронная доска объявлений. Система, которая в автоматическом режиме предоставляет некоторые услуги пользователям, подключающимся к ней через модем по телефонной линии. Основные услуги – передача файлов и почты. Часто являются также узлами в одной или нескольких электронных сетях, например, сети Fidonet. В таком случае пользователи BBS имеют доступ к услугам этих сетей.

В июне 1984 года вышла в свет седьмая версия программного обеспечения сети. Все стало предельно просто – создавался почтовый пакет, производился звонок, устанавливалась связь, и пакет передавался.

Идея и реализация Fidonet пришлась по душе операторам BBS, и начался интенсивный рост сети. В августе 1984 года в Fidonet было 30 телекоммуникационных узлов, в феврале 1985 года – 160, в начале 1987 года – 2000, в начале 1992 года – 20000, в феврале 1995 года – более 37000 узлов и т. д. Технология Fidonet оказалась столь популярной, что на ее основе созданы и функционируют несколько сотен любительских и коммерческих телекоммуникационных сетей, совместимых с Fidonet по программному обеспечению, а многие из них имеют шлюзы в Fidonet. Еще на самом начальном этапе развития в структуру адресов Fidonet была заложена иерархичность и многоуровневость, что позволило в дальнейшем разработать принципы децентрализованного управления и поддержки развития сети.

С момента возникновения Fidonet ее технологические стандарты разрабатывались самими членами сети. Вначале это были просто дополнительные возможности, вводимые создателями первых программ для Fidonet; однако со временем рост сети вызвал, с одной стороны, необходимость более жесткой стандартизации, а с другой стороны, постоянно росло количество предлагаемых членами Fidonet изменений и добавлений к технологиям. Для решения возникающих проблем был создан комитет FTSC[113], который за время своего существования разработал на основе многочисленных предложений членов сети несколько десятков стандартов различных компонентов технологии Fidonet. Эти стандарты носят общее название стандартов FTN[114]. Помимо коммуникационных проблем, решены также задачи криптографического шифрования передаваемых данных. Поэтому существует достаточно большое количество серьезных организаций, использующих программы, работающие по этим стандартам, для обмена данными между филиалами и головными офисами.

Появление Fidonet в России произошло весной 1990 года. В структуре адресов Fidonet заранее было зарезервировано адресное пространство для России, поэтому на всей территории страны сеть смогла развиваться как еди-

[113] FTSC – Fidonet technology standards comittee, комитет по стандартам технологии Fidonet.

[114] FTN – Fidonet technology network, сеть, работающая по стандартам Fidonet.

ное целое. В начале 1995 года в российском регионе Fidonet насчитывается более 1500 узлов, объединенных в 50 сетей по регионам. На 2005 год насчитывалось около 9000 узлов, объединенных примерно в 60 сетей по регионам.

Для того, чтобы достаточное количество телекоммуникационных узлов, объединенных в сеть, могли обмениваться информацией, необходимо наличие определенной структуры. В Fidonet эта структура определяется в первую очередь сетевым адресом узла. Адрес узла в Fidonet и любой FTN-совместимой сети имеет числовую форму и строится по следующей схеме:

`зона:сеть или регион/узел`

- *Узел* (*Node*) является наименьшей структурной единицей Fidonet; в то же время это основная единица Fidonet.
- *Сеть* (*Network*) – объединение узлов некой локальной географической области, обычно определяемое областью с удобной телефонной связью между узлами.
- *Регион* (*Region*) – это определенная достаточно крупная географическая область, включающая узлы, которые могут быть объединены в сети.
- *Зона* (*Zone*) – наиболее крупная структурная единица Fidonet, большая географическая область, включающая множество регионов и охватывающая одну или несколько стран и континентов. Fidonet насчитывает шесть зон: Северная Америка, Европа и территория бывшего СССР, Австралия и Океания, Южная Америка, Африка, Азия.

Таким образом, сетевая принадлежность конкретного узла, например 2:5049/25, определяется как узел 25 сети 5049 региона 50 зоны 2 Fidonet. Географическое местоположение узла также можно определить из сетевого адреса: 2 – Европа, 50 – Россия, 5049 – Казань.

С расширением Fidonet и ростом ее популярности появилось достаточно большое количество людей, стремящихся к общению в Fidonet, но не имеющих возможности поддерживать узел Fidonet. Для таких людей существует система *пойнтов*[115]. Пойнт, посылающий почту через определенный узел, пользуется адресом узла, к которому через точку добавлен номер пойнта, например 2:5049/25.1.

Существует разница между пойнтом и узлом. Пойнты не являются членами Fidonet, за их действия в сети несет ответственность узел, к которо-

[115] От английского *point* – точка.

му они подключены. Пойнт не обязан соблюдать технические процедуры, установленные для узла.

В Fidonet существуют свои правила (policy), сетевые и региональные координаторы, выбираемые обычно общим голосованием участников сети, а также писаные и неписаные законы.

2.8. Прочие сети

Помимо рассмотренных, в разное время существовали и существуют также следующие глобальные информационные сети:

- *MFENet* – Magnetic fusion energy network, сеть Министерства энергетики США, объединившая исследователей термоядерного синтеза с магнитным удержанием;
- *HEPNet* – High energy physics network, несколько сетей, объединяющих исследовательские центры, которые занимаются разработками в области ядерной физики и физики больших энергий;
- *SPAN* – Space physics analysis network, сеть NASA для ученых-астрофизиков;
- *CSNet* – Computer science network, сеть больших компьютеров, расположенных главным образом в США, но связанных с другими странами. Создана на субсидии NSF[116]. Сайты CSNET включали университеты, исследовательские лаборатории и некоторые коммерческие структуры; прекратила свое существование в 1991 году;
- *NSI* (NASA Science Internet) объединяет несколько компьютерных сетей по космическим исследованиям, физике космоса и другим научным направлениям в общую интерсеть глобального распространения. Сеть играла активную роль в формировании стратегии развития интернета и, в частности, в решении проблем совместимости протоколов TCP/IP с протоколами DECnet, OSI/ISO и прикладными протоколами для обработки адресной и структурированной числовой информации;
- *XNS* – Xerox network service или Xerox networking standard, сеть, по-

[116] NSF – National science foundation, Национальный научный фонд США.

строенная на протоколах, разработанных XPARC[117]. Позволяет пользователям использовать файлы, расположенные на другом компьютере. Предвестник протоколов IPX и NETBIOS;

- *RUNNet* – Russian university network, отраслевая телекоммуникационная сеть Министерства образования и науки с точками присутствия во многих городах России. Образована в рамках государственной научной программы «Университеты России» в 1994 году. Ее магистральная часть содержит узлы в Москве, Петербурге, Новосибирске, Екатеринбурге, Ростове-на-Дону, кроме того, к ней подключены региональные подсети. Центр сети находится в Санкт-Петербурге;
- *RBNet* – Russian backbone network, создана в 1996 году в рамках Межведомственной программы «Создание национальной сети компьютерных телекоммуникаций для науки и высшей школы». В настоящее время выполняет интегрирующую роль в обеспечении единого информационного пространства науки и образования РФ. Сеть RBNet построена как базовая транспортная магистраль, обеспечивающая связность многочисленных сетевых сегментов, которые обслуживают различные группы пользователей, относящихся к сфере науки и образования РФ. С технологической точки зрения она представляет собой высокоскоростную IP-сеть, объединяющую федеральные округа с подключенными к ней региональными сегментами сетей науки и образования. Вся инфраструктура охватывает около 50 регионов РФ. Подключения к сети осуществляются на базовых узлах, расположенных в Москве, Санкт-Петербурге, Ростове-на-Дону, Самаре, Нижнем Новгороде, Казани и некоторых других городах. Оборудование RBNet размещается, как правило, на региональных предприятиях связи, что обеспечивает надежное круглосуточное обслуживание. RBnet – сеть академическая, причем ориентированная на Россию, поэтому международная связь в ее пределах осуществляется не приоритетно.

В настоящее время магистральную инфраструктуру RUNNet/RBNet использует большинство российских научно-образовательных сетей (FREENet, MSUnet, Radio-MSU, RASnet, Relarn-IP, региональные научно-

[117] XPARC – Xerox Palo Alto research center, исследовательский центр корпорации Xerox в Пало-Альто (штат Калифорния), в котором выполнено множество важнейших для компьютерной индустрии разработок. В частности, там велись работы по созданию графического интерфейса, реализована идея компьютерной мыши и т. д. Основан в 1969 г.

образовательные сети), пользователями которых являются государственные и негосударственные высшие учебные заведения, институты РАН, государственные научные центры, федеральные и региональные учреждения культуры, учреждения общего среднего и дополнительного образования, различные некоммерческие организации;

- *Голден Телеком* – это сеть интегрированных телекоммуникационных услуг и услуг Интернет крупнейшего коммерческого оператора связи России и стран СНГ, охватывающая более 135 городов. Сеть построена на основе оптоволоконных линий и спутниковой связи и является частью трансевропейской IP-сети, связь с которой осуществляется на скорости до 2,4 Гбит/сек.;
- *Глобал Один* – составная часть всемирной сети Global One, созданной одноименной международной телекоммуникационной корпорацией. Сеть имеет узлы более чем в 200 городах на территории России;
- *GLASNET* существовала в России под эгидой «Ассоциации за прогрессивные коммуникации», в рамках которой действовали несколько некоммерческих компьютерных сетей гуманитарно-экологического характера: PeaceNet, EcoNet, GreenNet, Comlink и ряд других. По состоянию на март 1993 года в рамках АПК было объединено 11 сетей, 17 тысяч организаций и частных лиц из 94 стран. Основная служба GlasNet других сетей АРС – электронная почта. Пользователям предоставлялась возможность участвовать в более чем 1200 тематических конференциях по проблемам молодежи, разоружения, образования, окружающей среды, прав человека, здравоохранения, региональной политики, демографии и тому подобное;
- *гражданская сеть (ГС) Республики Татарстан* создана в 1994 году на базе Казанского государственного университета (КГУ) совместно с Казанским научным центром РАН (КНЦ РАН) и рядом вузов Казани (один из авторов данного пособия в 1994-1999 годах принимал участие в данном проекте). Это крупная телекоммуникационная система регионального масштаба, объединяющая более 130 организаций. С технической точки зрения ГС представляет собой совокупность опорных узлов, расположенных на телефонных станциях города и в КГУ, к которым при помощи арендуемых линий связи подключены локальные сети организаций-участников. В сети используются технологии, обеспечивающие полную совместимость с интернетом. Фактически ГС является объединением на общей технической базе компьютерных

сетей вузов Казани, вузов в Набережных Челнах, академических институтов КНЦ РАН и Академии наук Республики Татарстан, республиканских больниц и клиник, организаций государственного управления, культуры и многих других некоммерческих организаций. Связь с соседними узлами интернета в Москве и Ульяновске обеспечивается через выделенные междугородние телефонные каналы. До появления ГС в Республике практически не было школ, библиотек, организаций здравоохранения, имеющих доступ в глобальные компьютерные сети;

- *SENet* – Science and education network, сеть научных и учебных организаций г. Казани, объединяет институты Казанского научного центра РАН, Академии наук Республики Татарстан, высшие учебные заведения города Казани. Образована в 2000 году Казанским научным центром РАН при финансировании РАН, фонда НИОКР РТ[118], РФФИ[119] и Федеральной целевой программы «Интеграция»[120]. Магистральная сеть, составляющая коммуникационную основу SENet, построена на двумегабитных медных frame relay линиях и 155-мегабитных оптоволоконных ATM-соединениях.

---

[118] Фонд научно-исследовательских и опытно-конструкторских работ, образован в 1993 г. с целью создания условий возникновения в Республике Татарстан конкурентоспособной экономики через реализацию инновационной политики развития производства. Инвестиционный потенциал Фонда НИОКР РТ формируется за счет ежеквартальных отчислений предприятий в размере 1,5% от себестоимости реализованной продукции и используется следующим образом: 1% (из общих 1,5%) остается в распоряжении предприятия для реализации собственных инновационных проектов, а оставшиеся 0,5% перечисляются в централизованную часть Фонда НИОКР в обязательном порядке. Процент, который остается на предприятии, должен быть использован на выполнение одного из мероприятий в соответствии с установленным перечнем. В случае неиспользования этой суммы или нецелевого использования эта часть также должна быть перечислена в централизованную часть Фонда. Часть централизованного фонда передается Академии Наук РТ. Она также используется для финансирования научно-технических и инновационных программ и кредитования разработок. Все виды финансирования осуществляются на конкурсной основе.

[119] РФФИ – Российский фонд фундаментальных исследований, самоуправляемая государственная организация, основной целью которой является поддержка научно-исследовательских работ по всем направлениям фундаментальной науки на конкурсной основе, без каких-либо ведомственных ограничений. Образован в 1992 г. в соответствии с указом Президента России. Ежегодно фонд финансирует проведение около 8 тысяч научных проектов, 300-400 научных конференций и десятки экспедиций, издание более 200 научных монографий и сборников и т. д.

[120] «Интеграция» – федеральная целевая программа, направленная на развитие и интеграцию вузовской и академической науки. Кроме того, в последние годы разворачиваются программы интеграции учебной, научной и производственной деятельности.

2.9. Интернет

Агентство DARPA начало работы в направлении разработки межсетевой технологии в середине 70-х, но архитектура и протоколы приняли современную форму лишь в 1977-1979 годах. В это время DARPA была известна как основное агентство, финансирующее исследования в области сетей с коммутацией пакетов, и внедрила множество новшеств в этой области в ARPANET. ARPANET использовала обычные выделенные линии точка-точка для соединения компьютеров, но DARPA также финансировала использование коммутации пакетов в радиосетях и спутниковых линиях связи. По существу, растущее разнообразие аппаратных сетевых технологий вынудило DARPA изучить межсетевое взаимодействие и продвинуться по направлению к объединенной сети.

2.9.1. Историческая линия развития сети интернет (Интернет, часть 2)

Объединенный интернет начал существовать с 1980 года, когда DARPA начала устанавливать на машинах, присоединенных к ее исследовательской сети, новые протоколы семейства TCP/IP. ARPANET вскоре после создания стал магистральной сетью нового интернета и был использован для большинства из ранних экспериментов с TCP/IP. Переход к технологии интернета был завершен в январе 1983 года, когда МО США установило, что все компьютеры, присоединенные к глобальным сетям, используют TCP/IP. В это же время ARPANET была разделена на две отдельные сети.

Для скорейшего распространения новых протоколов, их стали продавать по низкой цене. В это время большинство университетских факультетов компьютерных наук использовали версию операционной системы UNIX, разработанную в программном отделении Университета Беркли в Калифорнии, чаще называемую Berkeley UNIX или BSD UNIX. Создание реализаций протоколов TCP/IP для UNIX привело к возможности организации взаимодействия 90% компьютерных факультетов университетов. Новое программное обеспечение с протоколами появилось вовремя, так как в это время в университетах США шел процесс массового приобретения компьютеров и объединения их в локальные сети. Факультетам требовались протоколы взаимодействия, а других протоколов в общем пользовании в то время не было.

Помимо стандартных программ TCP/IP, решение Беркли предлагало набор утилит для работы с сетью, которые напоминали стандартные средства UNIX, используемые на одной машине. Главное преимущество утилит Беркли заключалось в их сходстве с обычным UNIXом. Сходство сетевых утилит с обычными системными и пользовательскими сыграло важную роль в распространении их среди пользователей UNIX.

UNIX Беркли обеспечивала новую абстракцию операционной системы, известную как порт (socket), которая позволяла прикладным программам получать доступ к коммуникационным протоколам. Порт получил опции для нескольких типов сетевых протоколов, помимо TCP/IP, поскольку являлся абстракцией на уровне операционной системы. Введение порта было очень важным, так как позволяло программистам использовать протоколы TCP/IP с минимумом затрат.

Успех технологии TCP/IP и интернета в университетской среде вынудил другие группы тоже использовать его. Начиная с 1985 года, началось создание сетей на основе суперкомпьютерных центров. В 1986 году открылось финансирование глобальной магистральной сети, названной NSFNET, которая впоследствии связала между собой все суперкомпьютерные центры и ARPANET.

Использование протоколов TCP/IP и рост интернета не ограничивались проектами, финансирующимися правительством. Основные компьютерные корпорации присоединились к интернету, так же как и множество других больших корпораций, включая нефтяные компании, автомобильные концерны, электронные фирмы и телефонные компании. Вдобавок, многие компании используют протоколы TCP/IP в своих внутренних сетях, даже если они не присоединены к объединенному интернету.

Быстрое расширение привело к проблемам диапазонов, непредусмотренным в исходном проекте, и заставило разработчиков найти технологии для управления большими, распределенными ресурсами. В исходном проекте, например, имена и адреса всех компьютеров, присоединенных к интернету, хранились в одном файле, который редактировался вручную и затем распространялся по всему интернету. Но в середине 1980 года стало ясно, что центральная база данных неэффективна. Во-первых, запросы на обновление файла превышали возможности людей, обрабатывавших их. Во-вторых, даже если существовал корректный центральный файл, не хватало пропускной

способности сети, чтобы позволить либо частое распределение его по всем местам, либо оперативный доступ к нему из каждого места.

Были разработаны протоколы DNS (см. параграф 1.21), и стала использоваться система имен по всему объединенному интернету, которая позволяет любому пользователю автоматически определять адрес удаленной машины по ее имени.

В течение семи лет после своего создания интернет объединил сотни индивидуальных сетей, размещенных в США и Европе. Он соединил почти 20000 компьютеров в университетах, правительственных и частных исследовательских лабораториях. Как размер, так и использование интернета продолжали расти быстрее, чем предполагалось. К концу 1987 года его рост достиг 15% в месяц и оставался таким в течение двух лет. В 1990 году интернет включал более 200000 компьютеров. Сегодня встала проблема перенасыщения доступного адресного пространства интернета, предусмотренного действующей версией протоколов TCP/IP – IPv4. Это пространство позволяет одновременно находиться в одной сети более чем двум миллиардам устройств. При учете разделения на подсети (не пересекающиеся друг с другом) это число увеличивается минимум вдвое. Тем не менее, резкое увеличение категорий и количества устройств, способных подключаться к интернету привело к тому, что момент исчерпания адресного пространства уже не за горами. Поэтому в настоящее время идет переход на IPv6 протоколов TCP/IP, который надолго снимет проблему перенаселения сети.

24 октября 1995 года FNC единодушно одобрил резолюцию, определяющую термин «интернет». Это определение разрабатывалось при участии специалистов в области сетей и в области прав на интеллектуальную собственность.

Как следует из резолюции, FNC признает, что следующие словосочетания отражают определение термина «интернет».

Интернет – это глобальная информационная система, которая:

- логически взаимосвязана пространством глобальных уникальных адресов, основанных на Internet-протоколе (IP) или на последующих расширениях или преемниках IP;
- способна поддерживать коммуникации с использованием семейства TCP/IP или его последующих расширений/преемников и/или других IP-совместимых протоколов;

• обеспечивает, использует или делает доступными на общественной или частной основе высокоуровневые услуги, надстроенные над описанной здесь коммуникационной и иной связанной с ней инфраструктурой.

За два десятилетия своего существования интернет претерпел кардинальные изменения. Он зарождался в эпоху разделения времени, но сумел выжить и во времена господства персональных компьютеров, одноранговых сетей, систем клиент-сервер и сетевых компьютеров. Он проектировался до первых локальных вычислительных сетей (ЛВС), но впитал эту новую сетевую технологию, равно как и появившиеся позднее технологии коммутации ячеек и кадров. Он задумывался для поддержки широкого спектра функций, от разделения файлов и удаленного входа до разделения ресурсов и совместной работы, породил электронную почту, а чуть позже – Всемирную паутину, которая сегодня ошибочно с ним отождествляется. Но важнее всего то, что Сеть, создававшаяся вначале как объект деятельности небольшого коллектива исследователей, выросла до коммерчески выгодного предприятия, в которое ежегодно вкладываются сотни миллиардов долларов.

В настоящее время интернет объединяет более 100 тысяч сетей, 200 млн. пользователей и 5 млн. узловых компьютеров более чем в 150 странах мира. Интернет не принадлежит и не является собственностью какой-либо организации. Фактически это кооперация независимых сетей, в каждой из которых имеется собственная администрация и свои процедуры административного управления.

Не следует думать, что все изменения интернета остались позади. По названию и географически интернет является сетью[121], но это порождение компьютерной, а не традиционной телефонной или телевизионной индустрии. Чтобы передовой уровень интернета сохранялся, изменения должны продолжаться, причем в темпе, присущем компьютерной индустрии.

Происходящие в наши дни изменения направлены на предоставление таких услуг, как передача данных в реальном масштабе времени с целью поддержки, например, аудио- и видеопотоков. Повсеместная доступность сетей в сочетании с мощными, компактными и доступными по цене вычислительными и коммуникационными средствами делает возможным построение совершенно новых способов мобильных вычислений и коммуникаций.

[121] Internet – «междусеть».

Для будущего интернета важнее всего даже не то, как будут меняться технологии, а то, как будет управляться сам процесс изменения и развития. Архитектура интернета ранее определялась ядром, состоящим из ведущих проектировщиков, но с увеличением числа заинтересованных сторон форма ядра изменилась. Успех интернета расширил круг людей и организаций, вкладывающих в него финансовые и интеллектуальные ресурсы. Споры вокруг управления доменным пространством имен и формата следующего поколения IP-адресов показали, что идет поиск новой социальной структуры, способной осуществлять руководство интернетом в будущем. В то же время, промышленные круги нуждаются в экономическом обосновании крупных инвестиций, необходимых для будущего роста, например, в плане улучшения технологии доступа к сети. Если интернету суждено столкнуться с неудачами, это произойдет не из-за дефицита технологий, предвидения или мотивации. Главная опасность состоит в сложности социальной, в том, что мы сами не можем установить единое направление и решить, каким же путем двигаться в дальнейшее светлое или, наоборот, темное будущее.

2.9.2. История интернета в России

В Россию интернет впервые проник в начале 90-х годов. Ряд университетов и исследовательских институтов приступили в это время к построению своих компьютерных сетей и обзавелись зарубежными каналами связи. Особенно следует отметить Институт атомной энергии им. Курчатова. На базе ИАЭ сложились две крупнейшие коммерческие компании, предоставляющие услуги по подключению к интернету – Релком и Демос, а также Российский институт развития общественных сетей. В дальнейшем РОСНИИРОС стал головной организацией, координирующей развитие российской части интернета.

До 1993 года Релком был фактическим монополистом на рынке сетевых услуг и предоставлял своим пользователям в основном электронную почту. Собственно, это еще не было интернетом, хотя уже являлось компьютерной сетью – для пересылки сообщений использовались не интернет-протоколы, а более старый протокол UUCP. Монопольное положение Релкома с неизбежностью приводило к высокому уровню цен на его услуги.

В 1993 году мощный импульс развитию интернета в России придала «Телекоммуникационная программа» Международного научного фонда.

Программа финансировалась Джорджем Соросом[122] – известным американским мультимиллионером и филантропом. Еврей венгерского происхождения, Сорос на собственном опыте познакомился с особенностями тоталитарных режимов и считал, что распространение интернета в бывших социалистических странах поможет им преодолеть сложившуюся информационную изоляцию. По программе «Интернет» фондом Сороса на базе классических университетов России были организованы интернет-центры.

Влияние инициатив Сороса на развитие интернета в России очень велико и не ограничивается прямыми результатами его проектов. С одной стороны, благодаря авторитету Сороса в международных финансовых кругах в российской отрасли связи была создана благоприятная атмосфера для зарубежных инвестиций, которая сохранялась до финансового кризиса августа 1998 года. С другой стороны, эта деятельность способствовала пониманию важности интернета российскими государственными структурами.

Медленно, но верно в правительстве начали осознавать, что только развитие Интернета способно до некоторой степени приостановить утечку мозгов из России и сохранить здесь высшее образование мирового класса. В 1994 году в рамках государственной научной программы «Университеты

---

[122] Джордж Сорос (род. 1930) – американский финансист, инвестор и филантроп. Сторонник теории открытого общества и противник «рыночного фундаментализма». Его деятельность вызывает неоднозначную оценку в разных странах и различных кругах общества. Свое состояние (ок. 7 млрд. долл. США) Сорос заработал с помощью игр на понижение курсов акций, в ходе которых он использовал свою «теорию рефлексивности фондовых рынков». Согласно этой теории, решения о покупках и продажах ценных бумаг принимаются на основе ожиданий цен в будущем, а поскольку ожидания – категория психологическая, она может быть объектом информационного воздействия. Атака на валюту какой-либо страны состоит из последовательных информационных ударов через СМИ и аналитические издания, сочетающихся с реальными действиями валютных спекулянтов, расшатывающих финансовый рынок.

В 1979 году Джордж Сорос создал в США благотворительный фонд «Открытое общество» (Open society fund). В США его структуры осуществляют целый ряд проектов, самым масштабным из которых является борьба за легализацию наркотиков и широкое внедрение в медицинскую практику марихуаны и метадона.

В 1988 году в СССР Сорос организовал фонд «Культурная инициатива» в поддержку науки, культуры и образования. Позднее фонд был закрыт, так как деньги использовались в личных целях определенных лиц. В 1995 году в России был организован новый фонд «Открытое общество». С 1996 по 2001 год Фонд Сороса вложил в проект «Университетские центры Internet» около 100 миллионов долларов, в результате чего на территории России появились 33 интернет-центра.

В конце 2003 года Сорос официально свернул свою благотворительную деятельность в России. В 2004 году «Открытое общество» перестало выдавать гранты. Но созданные при содействии Фонда Сороса структуры активно работают и в настоящее время.

России» было выделено направление по созданию федеральной университетской компьютерной сети RUNNet. В 1996-98 годах была построена опорная сеть для нужд науки и высшей школы RBnet, использовавшая волоконно-оптические каналы большей емкости. Она финансировалась уже отдельной строкой государственного бюджета.

Одновременно возникали и быстрыми темпами развивались сети коммерческих поставщиков услуг Интернета. Они образовывались как акционерные общества с чисто российским или смешанным капиталом на базе крупнейших предприятий транспорта и связи. Вначале эти сети ориентировались в основном на подключение организаций, таких, как банки, государственные учреждения и средства массовой информации. Затем они стали все шире обслуживать частных пользователей там, где существовал платежеспособный спрос, в первую очередь в Москве и Санкт-Петербурге. Были организованы пункты обмена трафиком коммерческих сетей между собой и с академическими сетями. Электронная почта перестала ходить из одного района Москвы в другой через Америку, что часто наблюдалось ранее[123].

В настоящее время коммерческие компании, предоставляющие доступ в интернет, составляют мощный и быстроразвивающийся сектор российской экономики с высоким уровнем конкуренции. В 1998 году Ростелеком, российский монополист международной и междугородней телефонной связи и владелец большей части российских волоконно-оптических каналов, организовал сеть «Ростелеком–Интернет», бурно развивавшуюся, благодаря дешевизне и агентской схеме развития. На сегодняшний день это крупнейший поставщик услуг интернета в России.

В конце 1998 года в России было около 1,5 миллиона пользователей интернета, больше половины которых проживало за пределами Москвы. В 1999 году число российских пользователей Сети превысило 5 миллионов, в 2001 году – 9 миллионов, на конец 2006 года это число составляло 25,8 миллиона человек. По доле от всего населения это примерно соответствует уров-

[123] Как было рассмотрено в первой главе настоящего пособия, при установлении соединений для передачи выбирается наиболее свободный маршрут. При отсутствии высокоскоростных широкополосных каналов связи между абонентами, даже если они располагаются в соседних зданиях, соединение может быть установлено таким образом, что пакеты преодолеют расстояние, в десятки раз большее расстояния между абонентами. Таким образом, было действительно нередким случаем установление соединения через США. Если учитывать, что стоимость трафика при передаче за рубеж существенно возрастала, услуги на подключение к сети были весьма недешевы.

ню Латинской Америки и в несколько раз меньше, чем в ведущих в коммуникационном отношении странах (государства Западной Европы, США, Канада, Австралия, Великобритания, скандинавские страны), хотя и заметно больше, чем в Африке, Индии и Китае. Несмотря на затянувшийся кризис, интернет в России в последние годы развивается такими же высокими темпами, как и во всем мире. В настоящее время интернет вышел за пределы крупных городов и распространился до уровня районных центров, а по количеству пользователей Москва соответствует развитым европейским странам (в ноябре 2006 г. доступ в интернет имели ок. 44% москвичей).

При благоприятных условиях русская аудитория может оказаться значительно больше, например, немецкой. В России уже представлено большинство разновидностей интернет-сервисов. Российская аудитория интернета, если не считать количества и абсолютного уровня доходов, по остальным параметрам практически не отличается от западной. Типичные пользователи Web-сервисов относятся к активному в социальном и экономическом отношении слою населения и склонны к поиску новых возможностей для развития личности и бизнеса.

К основным проблемам российских пользователей можно отнести, в первую очередь, отсутствие развитых систем телекоммуникации и низкое качество телекоммуникационных услуг. Высокоскоростное и качественное соединение, позволяющее использовать весь потенциал интернета, российскому пользователю обходится недешево. Хотя в последнее время наблюдается значительное изменение в этой области в связи с развитием широкополосного безлимитного обслуживания на основе абонентской платы (например, «Стрим» в Москве).

2.9.3. Основные сервисы интернета

Под интернетом подразумевается совокупность сетей, базирующихся на IP-технологии обмена данными и обеспечивающих пользователям наивысшую степень комфорта на коммутируемых или выделенных линиях: высокие скорости, работу с электронной почтой и предоставление самых современных услуг, в числе которых центральное место занимает WWW-технология.

К основным используемым в нынешнем интернете службам можно отнести следующие:

- WWW;
- электронную почту;
- FTP-серверы и файловые архивы;
- конференции Usenet;
- интернет-пейджеры ICQ и IRC;
- файлообменные сети;
- факсимильные услуги.

Самая популярная служба интернета – WWW. Подавляющее число серверов ориентировано именно на эту службу. Подробнее служба WWW и ее основной протокол HTTP рассматривались в предыдущей главе. Префиксы, используемые этой службой в адресах интернета: http, https[124].

Другая служба интернета, электронная почта, является электронным аналогом обычной почтовой службы. Аналогии можно провести во многих пунктах, вплоть до наличия почтового ящика (у пользователя) и почтового отделения (сервера). Почтовая служба делятся на три части:

- SMTP-служба, для отправления заранее подготовленной почты;
- POP3-служба, для получения почты;
- IMAP-служба, совмещающая в себе первые две, но подразумевающая непосредственную работу с почтой без отсрочки во времени.

Первые две службы обычно действуют взаимосвязанно, а при использовании третьей они могут быть и не востребованы.

Почтовый адрес пользователя в интернете должен быть составлен в соответствии с одним из следующих форматов:

<имя пользователя>@<адрес компьютера>

<адрес компьютера>#<имя пользователя>

Наиболее распространен первый формат. В действительности, большинство почтовых клиентов в настоящее время поддерживают только его, а знак «@»[125] приобрел специфическое значение признака электронного адреса.

---

[124] HTTP Secured – защищенный протокол HTTP для передачи криптографически закрытых данных. Получает все большее распространение в связи с развитием онлайновых платежных систем. Обычно используется совместно с SSL.

[125] В английской традиции знак «@» произносится как «at». Происхождение символа довольно древнее и, по последним сведениям, ведет свое начало от древнегреческих виноторговцев, использовавших этот символ для отмечания амфор с вином. Отечественное наименование «собака» также имеет интересное происхождение. В 1980-е годы, когда были распространены компьютерные игры, использовавшие текстовый режим монитора,

Рассмотренная выше адресация компьютеров должна обеспечивать уникальность адреса каждого компьютера. Обеспечить же уникальность имени пользователя гораздо проще. В общем случае, формат почтового адреса подразумевает, что один компьютер может быть использован и несколькими пользователями, имена которых должны различаться. Широкое распространение на практике получило также использование нескольких имен для одного пользователя.

Так как электронная почта (не обязательно с адресацией описанного формата) используется не только в интернете, но и в других компьютерных сетях, отметим, что в именно интернете она отличается расширенными возможностями и повышенной оперативностью, превращающей ее фактически в экспресс-почту. Для работы с ней используются почтовые программы: Microsoft Outlook, The Bat!, Silphyd, Eudora, The Bee и т.д.

Префикс, используемый этой службой в интернете (используется для маскировки, так как непосредственная работа осуществляется по отдельным информационным потокам): mailto.

Служба FTP-серверов сегодня редко используется как самостоятельный сервис. Дело в том, что FTP-архив представляет собой массив большого объема файловой информации, но практически без каких-либо комментариев и лишенный поисковой системы. Поэтому FTP-сервера обычно используются совместно с WWW, на базе которого реализуются поисковая система, аннотации и пр. Кроме того, через FTP зачастую организуется административная работа с внутренним содержимым WWW-сайта.

При работе с FTP для получения файлов может быть достаточно программы-браузера, но при двустороннем взаимодействии обычно требуется специализированная программа – FTP-клиент, например: CuteFTP, AceFTP, FlashFXP, Wget и др.

Службой FTP в интернете используется префикс ftp.

Весьма эффективными информационными службами являются конференции Usenet. Телеконференции долгое время являлись одним из основных средств оперативного обсуждения проблем и средствами получения квалифицированных консультаций. Но в последнее время эта роль все больше пе-

---

некоторые элементы игрового интерфейса строились на условностях. Так, в одной из наиболее популярных игр главный герой отображался в виде буквы «М», его жена – буквы «Ж». Домашнее животное получило условное обозначение «@».

реходит к так называемым форумам, работающим на базе службы WWW.

Для пользования услугами, предоставляемыми службой Usenet, требуется программа, понимающая протоколы этой службы. В некоторых почтовых программах такая возможность реализована, например, Microsoft Outlook, но есть и программы, разработанные специально для работы с Usenet.

Префикс, используемый этой службой: news.

В последнее время в интернете очень популярны так называемые интернет-пейджеры. Самым ярким представителем этого рода услуг является сервис ICQ (подробнее см. параграф 2.10.1). Существуют также аналоги ICQ – MSN, AIM, Trillian, Odigo и другие. Для работы с ними нужны соответствующие программы-клиенты. Некоторые такие программы понимают несколько протоколов связи и позволяют объединить в одном пространстве несколько сетей.

Префикса в интернете у этих служб нет, поскольку они пользуются уже существующими информационными потоками.

Другая сеть, IRC (Internet relay chat), также позволяет общаться в реальном времени. В этой сети существует ряд условностей и правил взаимодействия, что привело к тому, что в последнее время она слабо развивается. В общих чертах она схожа с телеконференциями Usenet, но позволяет также обмениваться большими объемами информации и предоставляет другие услуги. Для работы с IRC используются специальные программы, но их довольно мало, например, для Windows существует только один популярный клиент – mIRC. Это не значит, что данная программная область неинтересна для разработки, просто mIRC исчерпывает все потребности.

Префикс службы: irc.

2.10. Глобальные сети на базе P2P

В 1996 г. израильские программисты разработали программу ICQ, тем самым показав возможность быстрой непосредственной связи между двумя произвольными пользователями интернета. Спустя три года появился сервис под названием Napster, каталогизировавший доступные файлы пользователей и реализовавший поиск в каталогах. Посредством такого поиска оказалось возможным найти интересующий файл у другого пользователя и напрямую с его компьютера скачать этот файл. Так появились файлообменные сети, час-

то обозначаемые как peer-to-peer (отсюда появилось наименование «пиринговые сети» и понятие «пиринговые технологии»), или P2P[126]. Интерес к ним сильно возрос, когда возник конфликт между Napster и звукозаписывающими компаниями. Стали появляться подобные ей сети причем обмен данными уже не ограничивался лишь аудиофайлами.

Четкого определения P2P нет. Два наиболее распространенных следующие:

1. P2P – это технология построения распределенной сети, где каждый узел может одновременно выступать как в роли клиента (получателя информации), так и в роли сервера (поставщика информации). Как правило, сеть состоит из равноправных узлов, причем каждый из них взаимодействует лишь с некоторым подмножеством узлов сети, так как установление связи «каждый с каждым» невозможно из-за ограниченности ресурсов (как вычислительных, так и пропускных). При этом передача информации между узлами, не связанными в данный момент непосредственно, может осуществляться как от узла к узлу, так и путем установления временной прямой связи. Все вопросы маршрутизации и авторизации сообщений, передаваемых по эстафете, лежат не на едином сервере, а на всех этих отдельных узлах. Такое определение также известно под названием «pure P2P».

2. Более общее определение. P2P – это класс приложений, совместно использующих распределенные ресурсы (дисковое пространство и файлы, вычислительные ресурсы, пропускную способность и т. д.). К этому определению относятся следующие основные сервисы:

- файловые обменные сети (file-sharing networks). В данном случае сети P2P выступают хорошей альтернативой FTP-архивам, основной недостаток которых – ограниченность ресурсов и неспособность одновременного обслуживания неограниченного числа клиентов. P2P потенциально обладает целым рядом преимуществ: балансировкой нагрузки, более широкой полосой пропускания, высокой устойчивостью и широкими возможностями публикации;
- распределенные вычислительные сети, например, SETI@HOME. Этот проект продемонстрировал громадный вычислительный потенциал для хорошо распараллеливаемых задач. В настоящий момент в нем принимают участие более трех миллионов пользователей, а общее число «процессоро-

[126] P2P – peer-to-peer, равный к равному. Иногда эту аббревиатуру расшифровывают как «point-to-point» – то есть «точка к точке».

лет» перевалило за семьсот тысяч, и все это на абсолютно бесплатной основе, когда добровольцы не получают ничего, кроме красочного скринсейвера и возможности общественного признания;

- службы сообщений (Instant-messaging). Например, ICQ и AIM;
- сети групповой работы (P2P Groupware). Подобные приложения пока мало распространены, но развитие идет довольно интенсивно. Например, Groove Network – сеть, предоставляющая защищенное пространство для коммуникаций, OpenCola – технология поиска информации и обмена ссылками на наиболее интересные источники, где в роли поискового сервера выступает не бездушная железка, а каждый из пользователей сети. При ответственном подходе пользователей это обеспечивает гораздо более высокую релевантность, нежели при использовании автоматической поисковой системы.

Рассмотрим подробнее основные из перечисленных сервисов.

2.10.1. ICQ

Программа, названная ICQ[127], была разработана израильской компанией Mirabilis. Успех проекта был предопределен его инновационностью – ICQ не только стала первым в своем роде приложением категории IM[128], но и положила начало индустрии P2P-приложений. Однако успех ICQ стал следствием удачного сочетания многих факторов.

История ICQ начинается в июле 1996 года, когда четыре израильских программиста[129] поставили перед собой задачу разработать то, чего в интернете еще не существовало. Первые инвестиции в размере 12000 долларов в начинание сделал бизнесмен Йоси Варди, отец одного из программистов, не особо рассчитывая на успех[130].

Несмотря на то, что Интернет объединял миллионы пользователей по всему миру, связь между ними осуществлялась исключительно при участии серверов сети. Авторы ICQ решили дать пользователям возможность взаимо-

---

[127] Название является «игрой букв» – при произношении «ICQ» звучит очень похоже на английскую фразу «I seek you» – «Я ищу тебя». В просторечии – «Аська».

[128] IM – Internet (в другом варианте – Instant) Messenger, службы мгновенной доставки сообщений.

[129] Яир Голдфингер (Yair Goldfinger), 26 лет; Арик Варди (Arik Vardi), 27 лет; Сефи Вигизер (Sefi Vigiser), 25 лет; Амнон Амир (Amnon Amir) 24 года.

[130] Меньше, чем через два года Mirabilis была куплена корпорацией AOL за 287 миллионов долларов.

действовать непосредственно друг с другом. Восполнила пробел технология P2P, которая давала возможность пользователям интернета посылать сообщения друг другу, минуя сервер[131]. Можно сказать, что она позволила связывать компьютеры пользователей напрямую, минуя DNS-серверы и создавая собственные «не-DNS» адреса в сети. Mirabilis стала первой компанией, предложившей использовать эту технологию для организации системы мгновенной связи, и положила начало развитию новой индустрии в сети.

Первая версия ICQ появилась 15 ноября 1996 года. Спустя всего полгода ICQ получило право называться самой большой всемирной онлайновой коммуникационной сетью: в системе зарегистрировался миллионный пользователь.

Новизна сервиса обмена мгновенными сообщениями играла немаловажную роль, однако была далеко не единственной причиной стремительного распространения программы в интернете. Mirabilis первой применила уникальную технологию распространения, которая давала возможность пользователям самим распространять программу. Это оказалась не просто технология, а целая философия, связанная с путями, которыми люди сообщают друг другу информацию и убеждают воспользоваться теми или иными возможностями новых технологий, и получившая впоследствии название «вирусный маркетинг»[132]. Суть этого маркетинга заключается в том, что информация распространяется подобно вирусам – каждый пользователь услуги может являться генератором и отправителем рекламной информации о продукте, сообщая знакомым о желании пообщаться с ними при помощи ICQ.

Расчет был прост. Интернет-пейджер абсолютно бесполезен, если ваши корреспонденты не имеют к нему доступа. Следовательно, вы сами начнете сообщать им о его существовании и убеждаете установить необходимое программное обеспечение. Mirabilis сделала ставку именно на мотивацию пользователей распространять информацию об ICQ. Она понимала, что, если ICQ придется по душе пользователям, те обязательно найдут возможность продвинуть сервис. Именно поэтому творцы ICQ прилагали все усилия, чтобы сделать распространение продукта максимально легким. Например, использовалась стандартная электронная почта для рассылки приглашений присое-

[131] Первоначально такая технология называлась «server-less email».

[132] В настоящее время принято название «сетевой маркетинг». Под этим подразумевается такая форма организации распространения некоторой продукции, когда пользователь в силу тех или иных причин сам становится ее распространителем и популяризатором.

диниться к ICQ. Немаловажным был и тот факт, что программное обеспечение являлось бесплатным и доступным – его можно было свободно загрузить с сайта ICQ или специальных порталов.

При этом Mirabilis поначалу практически полностью игнорировала традиционные методы продвижения продукта.

Ставка на вирусный маркетинг оказалась верной. Пользователи, с энтузиазмом встретившие ICQ, самостоятельно распространяли приложение, привлекая к общению посредством IM своих друзей и знакомых. Благодаря этому ICQ быстро достигла рекордных показателей загрузки программы в истории интернета. Все это свидетельствовало об исключительной важности категории программного обеспечения, созданного Mirabilis – программ мгновенной доставки сообщений.

Mirabilis занимала монопольное положение до мая 1997 года, за это время количество зарегистрированных пользователей достигло 850 тысяч. Первым конкурентом ICQ стал продукт компании America OnLine[133] – AOL AIM. Будучи самым крупным интернет-провайдером в США, компания America OnLine выбрала достаточно агрессивную стратегию вывода на рынок собственного интернет-пейджера. При подключении к интернету каждый пользователь получал возможность скачать AIM вместе с 500 часами работы в интернете бесплатно. Благодаря этому программа получила в США широкое признание.

Успех ICQ дал толчок интенсивному развитию P2P-индустрии. В мае 1998 года Yahoo! выпустила «Yahoo! Pager», в июле 1999 года Microsoft создала «Microsoft Messenger» на базе MSN[134]. Впрочем, появление конкурентов не помешало Mirabilis удержать доминирующее положение в созданном сегменте.

Сохранение лидирующих позиций во многом оказалось возможно благодаря избранной стратегии. Mirabilis повела ICQ по пути постоянного развития и обновления. В июне 1997 г. ICQ достигла нового рекорда – одновременно в режиме online общались 100 тысяч пользователей. Интенсивные темпы развития позволили ICQ в течение 1998 года более чем в пятнадцать раз увеличить количество пользователей более чем в 15 раз и заключить беспрецедентную сделку. В июне 1998 г. компания Mirabilis была приобретена главным конкурентом – компанией America OnLine за 287 млн. долларов.

[133] См. параграф 2.11.
[134] MSN – Microsoft Network.

Причин, побудивших компанию AOL, которая уже имела собственный IM, купить маленькую израильскую компанию за столь крупную сумму, было несколько. Во-первых, количество пользователей ICQ достигло 16 миллионов. Хотя на тот момент ни Mirabilis, ни AOL не имели точного представления, как можно заработать при помощи ICQ, возможность доступа к такой массовой аудитории была очень привлекательна. Во-вторых, исключительной особенностью ICQ оставалось то, что это было первое приложение класса IM в истории сети. Однако главное преимущество перед AIM заключалось в том, что 60% пользователей ICQ находились вне США, тогда как AIM практически не имел клиентов за границами страны.

Став собственностью AOL, компания, переименованная в Mirabilis LTD, продолжала поддерживать марку лидера. Была создана мощная поисковая система, разработаны версии ICQ для операционных систем Mac OS X и Unix/Linux. Появились приложения-конкуренты, эксплуатирующие тот же протокол, что и оригинальная программа (среди них можно выделить наиболее удачные разработки – Miranda IM, &RQ, QIP). Развитие ICQ продолжается и в настоящее время. Из приложения, позволяющего всего лишь отправлять сообщения в интернет, ICQ переросла в крупный комплекс инструментов связи и информации.

Кроме того, в ноябре 2001 года появилась версия ICQ, которая предоставляла доступ ко всем функциям ICQ посредством браузера, и не требовала наличия самого ICQ-клиента. Веб-приложение в первую очередь рассчитано на тех, кто часто путешествует или постоянно использует несколько ПК, например, дома и на работе.

2.10.2. Технологии ICQ

На сегодняшний день существуют больше десяти версий клиента ICQ. Каждый из них работает на своей версии ICQ-протокола, номер которой обычно совпадает с версией клиента. Однако базовых версий всего две:

- протокол, работа которого основана на протоколе UDP;
- протокол, работа которого основана на протоколе TCP.

Техническая история ICQ начиналась с протокола UDP, на нем были реализованы версии протоколов с первого по пятый. Им соответствовали клиенты ICQ97, ICQ98, ICQ99. Поскольку в них применялся протокол UDP, то постоянного соединения клиент–сервер не создавалось. Передача осуще-

ствлялась по принципу: «пакет передал – получил подтверждение; если подтверждения не получил, то передал повторно».

На сегодняшний день эти версии протоколов почти не поддерживаются. После поглощения Mirabilis корпорацией AOL в качестве основного протокола ICQ стал применяться уже используемый к тому времени протокол AIM, получивший новое воплощение в качестве второй основной версии ICQ-протоколов. Это и есть ICQ на базе TCP. Он включает в себя подверсии 7, 8 (OSCAR) и далее.

При подключении клиент ICQ должен пройти авторизацию на сервере по адресу **`login.icq.com:5190`**. Клиент соединяется с этим сервером и передает ему пакет, содержащий UIN[135] и пароль. Далее сервер присылает IP-адрес основного сервера и массив из 256 байт случайных данных, которые одновременно зеркалируются[136] на указанном сервере. Используя этот массив данных, клиент получает доступ к основному серверу и далее работает непосредственно с ним.

2.10.3. Napster

В сентябре 1999 года интернет-общественности была предложена небольшая бесплатная программа, спровоцировавшая впоследствии один из самых шумных скандалов за всю историю интернета. Автором программы был 19-летний студент Шон Фэннинг[137], также известный под прозвищем Napster[138]. Программа тоже получила название «Napster».

Как и множество других любительских проектов, изначально сеть обмена файлами Napster предназначалась для «внутреннего использования» среди друзей и знакомых автора, однако довольно быстро сумела завоевать популярность сначала среди студентов многочисленных университетов, а потом и во всем мире. Уже спустя месяц начались инвестиции, примерно в то

---

[135] UIN – User identification number, уникальный идентификационный номер пользователя.

[136] Зеркалирование – создание полной копии файла или группы файлов на другом носителе. При изменении файлов на исходном носителе соответствующие изменения вносятся и в «зеркало».

[137] Шон Фэннинг (Sean Fanning) – член хакерской группы w00w00, занимающейся исследованиями в области безопасности Unix-систем. Автор нескольких сетевых утилит, таких как сканер портов napscan.c, генератор DDoS-атак orgasm.c и др.

[138] Napster – пушистик (разг. *англ.*).

же время была образована одноименная компания.

Принцип действия сети оказался прост до гениальности. Для успешного распространения файлов вовсе не обязательно, чтобы они были выложены на постоянно работающем сервере. Файлы могут храниться на компьютерах пользователей, а сервер будет лишь содержать информацию о том, какие именно компьютеры в данный момент включены, имеют доступ к сети и, соответственно, предоставляют эти файлы в общий доступ. Такая система позволяет не только экономить место, но и объединить в одну сеть огромное количество пользователей. Именно так и действовал Napster. С помощью специального клиента пользователи могли искать музыкальные файлы[139], хранящиеся в «расшаренных»[140] ресурсах других членов сети.

Вскоре количество скачанных музыкальных файлов стало измеряться тысячами, потом – десятками тысяч и миллионами. А потом у Napster начались проблемы. На компанию начали подавать в суд сначала музыканты (первой была группа «Metallica»), возмущенные бесконтрольным распространением их песен, а потом и Ассоциация звукозаписывающих компаний[141]. 12 февраля 2001 года деятельность Napster была прекращена по реше-

---

[139] Napster позволял обмениваться исключительно музыкальными файлами, причем преимущественно в формате MP3. Аббревиатура MP3 расшифровывается как MPEG Layer 3. MPEG – Motion picture expert group, экспертная группа по кинематографии. Это международная группа экспертов, занимающихся выработкой рекомендаций по обработке аудио- и видеоинформации. Они разработали серию рекомендаций по сжатию аудиоданных, названных Layer 1, 2 и 3 и отличающихся сложностью обработки сигнала. Непосредственно форматом MP3 занимались в западногерманском институте Fraunhofer и в компании Thomson. Их алгоритм сжатия аудиоданных был позже принят в качестве стандарта. Для преобразования аудиоданных в формат MP3 использовано так называемое перцептуальное кодирование, учитывающее психоакустические особенности человека при восприятии звука. Поскольку звуковой сигнал несет много избыточной информации, почти не различаемой человеческим ухом, ее при сжатии отфильтровывают с незначительным ущербом для качества звучания исходного материала.

Популярность MP3-формата обусловлена тремя факторами: бесплатным кодеком, опубликованным институтом Fraunhofer; сетью обмена музыкой Napster; программой-проигрывателем файлов, содержащих аудиоинформацию (в настоящее время также видео) WinAMP, написанной Джастином Франкелем из небольшой программистской компании Nullsoft.

[140] От английского «share» – делиться, разделять.

[141] RIAA – Recording industry association of america, Ассоциация индустрии звукозаписи Америки. Торговая группа, представляющая интересы звукозаписывающих компаний. На официальном сайте (www.riaa.com) отмечается, что члены RIAA производят более 90% всей аудиопродукции в США. В ее состав входит множество крупных, средних и мелких звукозаписывающих компаний, включая пять крупнейших – Sony, EMI, BMG, Universal и Warner Bros. Целью данной группы, по ее собственному утверждению, является защита интеллектуальных прав по всему миру.

нию апелляционного суда Северного округа Калифорнии. Апелляции и попытки добиться отмены судебного решения удовлетворены не были. В середине ноября 2002 г. оставшиеся активы и ресурсы Napster купила софтверная[142] компания Roxio.

29 октября 2003 года был открыт музыкальный интернет-сервис под названием Napster, предназначенный для онлайновой торговли файлами, содержащими аудиоконтент[143]. Однако к тому времени Napster уже утратил лидирующие позиции. Его нишу заняли другие файлообменные сети, число которых перевалило за несколько десятков.

2.10.4. Файлообменные сети

Файлообменные сети[144], с которыми чаще всего ассоциируется обозначение P2P (хотя сервисы мгновенных сообщений и распределенные вычислительные сети также относятся к этой технологии), обладают целым рядом преимуществ: балансировкой нагрузки за счет множества узлов, более широкой полосой пропускания, большой живучестью и широкими возможностями публикации.

Когда пользователь выходит в режим online, происходит подключение к какому-либо серверу, а в базе данных сервера отмечается, что абонент с таким-то номером доступен для связи. Благодаря единой или распределенной базе данных можно осуществлять поиск файлов или других пользователей.

Пользователь делает запрос об интересующем его файле, сервер производит поиск, генерирует ответ (список IP-адресов узлов, имена и размеры файлов) и отправляет его обратно абоненту. Тот выбирает, с какого узла загружать данные, соединяется напрямую с нужным узлом и закачивает этот файл, используя файлообменный протокол. После загрузки абонент инфор-

---

[142] «Софтверный» – от английского *software*, что означает «программное обеспечение». Софтверная компания – компания, занимающаяся разработкой, сопровождением и поддержкой программного обеспечения.

[143] Контент – от английского *content*, или содержимое. Это двоичный поток данных, передаваемых по сети в реальном времени, обычно до тех пор, пока не поступит какой-либо управляющий сигнал. Хотя термин часто употребляется в более общем смысле – как синоним информации, получаемой из интернета. *Аудиоконтент* – поток данных, содержащий аудиозаписи, *видеоконтент* – видеозаписи. *Медиаконтент* – объединяет в себе аудио- и видеосодержимое, при этом подразумевает возможность интерактивного взаимодействия с потребителем в реальном времени.

[144] File-sharing networks.

мирует сервер о результатах.

Все пиринговые технологии можно разделить на две категории:

- работа программ связана с операциями на центральном сервере. К этой категории относятся Napster, ICQ и, в усовершенствованном виде, некоторые другие, ныне действующие сети. Такие сети называются централизованными;
- все операции в сети осуществляются непосредственно между программами-клиентами. Промежуточные серверы для хранения информации специально не организуются, функции такого сервера выполняют сами клиенты. Это децентрализованные сети.

2.10.5. Централизованные пиринговые сети

Aimster

Aimster – один из первых пиринговых клиентов, в нем даже была предусмотрена возможность подключения к сети Napster. Внешне выглядел как нечто среднее между Napster и ICQ, поскольку позволял не только обмениваться файлами, но и общаться с другими пользователями. С помощью Aimster можно было обмениваться не только музыкальными, но и файлами других типов, например, видеоклипами или программами. Восстановление с прерванного места после обрыва связи не поддерживалось. Из параметров поиска можно было задавать минимальную скорость соединения, тип файла и минимальное приемлемое качество записи.

AudioGalaxy

Принцип работы AudioGalaxy отличался от принципа работы остальных программ. Чтобы найти нужный музыкальный файл, требовалось первоначально зарегистрироваться на сайте. Поиск происходил там же, требовалось выбрать нужные файлы из результатов поиска, затем клиент самостоятельно искал эти файлы и запускал их скачивание по мере обнаружения.

2.10.6. Децентрализованные пиринговые сети

Kazaa

Завоевавшая наибольшую популярность пиринговая сеть Kazaa работала по принципу распределенных узлов, называемых Supernodes (суперузлы), на которых находилась база с именами файлов и адресами узлов.

Под суперузлы выделяются наиболее мощные компьютеры с самым быстрым интернет-соединением. При запуске программы Kazaa на клиентском компьютере А происходит подключение к ближайшему суперузлу с пересылкой информации о том, какие файлы имеются для общего доступа на данном ПК.

Предположим, другой пользователь с компьютера В ищет некие данные. Он выполняет запрос, который перенаправляется на ближайший суперузел, получает от него информацию о том, где есть данный файл (это компьютер А), соединяется с ним напрямую и загружает файл. Предположим, пользователь на компьютере А выключает свой компьютер, загрузка при этом, естественно, прекращается. Клиент Kazaa пытается найти нужный файл на других клиентских узлах и, в случае положительного результата, продолжает закачку с прерванного места, но уже с другого компьютера. В противном случае загрузка возобновляется только при повторном подключении узла А. Если искомый файл присутствует сразу на нескольких машинах, клиентский модуль Kazaa разбивает его на фрагменты и загружает одновременно с нескольких узлов.

Сеть Kazaa работала[145] с любыми данными, наиболее популярными были музыка, видео и программное обеспечение. Клиент позволял использовать два режима поиска – простой и сложный, с детальным заданием критериев отбора.

iMesh

Файлообменная сеть iMesh (а также компания с одноименным названием) основана в 1999 году, через несколько месяцев после Napster. В противоположность последнему, iMesh позволяла находить и загружать файлы любого типа.

[145] Пока готовилось настоящее учебное пособие, суперузлы сети Kazaa были закрыты решением суда, а клиентское программное обеспечение удалено с сайта разработчика. Это фактически определило дальнейшую судьбу данной пиринговой сети.

Клиент, помимо файлообменных функций, предоставлял доступ к интернет-чату и форуму с большим количеством разделов. Но основным достоинством сети iMesh являлся очень быстрый поиск.

eDonkey

В отличие от Kazaa и iMesh, сеть eDonkey2000 не имеет центральных серверов и построена по принципу «среднего арифметического» между чистой P2P-технологией и клиент-серверной архитектурой.

В eDonkey2000 имеется множество серверов, и при регистрации пользовательские ПК подключаются к одному из них, который постоянно обменивается информацией с другими серверами eDonkey2000. То есть вместо одного центрального сервера здесь есть множество равноправных серверов. Клиентские узлы – это обычные компьютеры, на которые можно загрузить или отгрузить данные, в отдельных случаях они также могут выступать в качестве серверов.

Сервер служит средством соединения нескольких клиентов. Перекачка данных идет напрямую, без участия сервера. Вследствие децентрализации eDonkey2000 невозможно закрыть так, как это было сделано с Napster или Kazaa. Для этого необходимо отключить все серверы, а их список меняется ежедневно.

Отличительной чертой данной сети является система жестких ссылок на файлы. Это значит, что каждый файл, попадающий в пиринговую сеть, получает собственный цифровой идентификатор, основанный на подсчете контрольной суммы содержимого файла – так называемого хэш-кода. Такой подход позволяет избежать конфликтных ситуаций, когда одним и тем же именем названы несколько разных файлов, а также в определенной степени контролировать корректность загружаемого файла.

Все ссылки в системе eDonkey2000 выдаются в виде жестких ссылок, начинающихся с префикса «ed2k://». Таким образом, достаточно ввести ed2k-определитель, и клиентская программа сама начнет поиски нужного файла.

Gnutella

В 1999 году компания Nullsoft разработала протокол обработки и передачи запросов для файлообменных сетей под названием Gnutella. Однако

Nullsoft была куплена корпорацией AOL[146], и работа над Gnutella со стороны этой компании прекратилась. Однако проект продолжил развиваться самостоятельно.

Технология построения файлообменной сети Gnutella – это чистый peer-to-peer принцип. Центрального сервера здесь нет вообще, все задачи обработки и передачи запросов возлагаются на пользовательские компьютеры. По этой причине закрыть такую сеть принципиально невозможно, можно лишь пытаться воздействовать на нее.

Алгоритм работы Gnutella следующий. При первом запуске программы пользователь узла A вводит IP-адрес одного из других функционирующих узлов (узел B). Без адреса хотя бы одного из работающих в данный момент узлов пользователь не сможет подключиться к сети – это довольно важный момент. Далее программа посылает запрос узлу B на предмет подтверждения активности, и в случае позитивного ответа с компьютера A на B отсылается так называемый ping-запрос, который далее рассылается на другие компьютеры.

Узлы, получившие ping-запрос, посылают ответ, в котором содержится IP-адрес отправителя, номер порта и минимальная информация о файлах в фонде обмена. Когда ответы доходят до узла A, клиентская программа составляет список доступных узлов. Далее процедура традиционна – пользователь вводит запрос, и программа рассылает его для поиска файла всем узлам в списке. Каждый из них ищет в своем фонде указанный файл.

Если он найден, узел отсылает инициатору запроса ответ с информацией о файле и свой IP-адрес. На основании этих ответов программа выбирает один или несколько узлов, устанавливает с ним стандартное HTTP-соединение и загружает файл.

Grokster

В противоположность сетям типа Gnutella, в Grokster применена технология «FastTrack P2P Stack», призванная решить проблемы медленного поис-

[146] Покупка была обусловлена потребностью AOL в популярном и качественном медиаплеере, а Winamp, основная разработка Nullsoft, на тот момент практически определял законы индустрии программных медиаплееров. В то же время, концепция Gnutella шла абсолютно вразрез с политикой и принципами коммерческой AOL, поэтому разработка была свернута в кратчайшие сроки, тестовая версия программных компонентов для Gnutella пролежала на сайте Nullsoft менее двух недель. Однако джинн из бутылки уже был, что называется, выпущен. Компоненты незамедлительно появились на многочисленных сайтах, и разработка была продолжена энтузиастами.

ка и ограниченного количества найденных ссылок. Grokster – распределенная самоорганизующаяся сеть, в которой отсутствует центральный сервер. Эта структура многослойная, роли суперузлов в ней выполняют более мощные компьютеры.

Любой клиентский компьютер Grokster может стать суперузлом, если удовлетворяет требованиям аппаратной мощности и обладает надежным интернет-каналом. Управление сетью полностью автоматическое – суперузлы назначаются и аннулируются в соответствии с необходимостью без вмешательства администратора. За счет этого достигаются высокие скорость и результаты поиска.

2.10.7. Проблемы пиринговых сетей

Хотя все клиенты пиринговых сетей распространяются бесплатно, пользователю практически любой файлообменной сети приходится расплачиваться за это косвенно, просматривая рекламные сообщения, отображаемые на окне программы.

Кроме того, файлообменные сети, несмотря на неоспоримые преимущества, наносят значительный ущерб индустрии, в первую очередь – звукозаписывающей, хотя с каждым годом возрастает объем трафика, обеспечиваемый другими типами контента, большей частью – видео. Ежедневно через P2P прокачиваются терабайты записей известных поп-исполнителей в сжатых форматах, при этом часто они попадают в интернет еще до официального выхода альбома. Современные децентрализованные пиринговые сети совсем не просто контролировать и управлять потоками данных в них, а тем более закрыть. В случае с Napster закрытие центрального сервера привело к кончине сети, однако в той же eDonkey2000 единого сервера просто нет.

Звукозаписывающие компании США не смогли решить проблему простым закрытием сетей, поэтому были разработаны обходные способы влияния на пользователей пиринговых сетей. Во-первых, юристы RIAA заявили о своей готовности отслеживать наиболее активных участников P2P и преследовать их в судебном порядке. Во-вторых, была разработана технология распространения фальшивых файлов в пиринговых сетях. В-третьих, разрабатываются технологии подавления особо активных узлов пиринговой сети. Вариантов

здесь несколько – от DDoS-атаки[147] на этот узел до засылки «троянца»[148] под видом полезной программы, которая после попадания на пользовательский компьютер будет удалять все файлы подозрительных форматов. И не факт, что среди этих файлов не окажутся важные пользовательские документы.

2.10.8. Skype

27 июля 2004 года была выпущена первая финальная версия интернет IP-телефона Skype. Этому предшествовал более чем годовой срок тестирования технологии, поэтому к официальному представлению она оказалась уже достаточно проработанной. Идея Skype заключается в организации бесплатной глобальной телефонной связи высокого качества, базирующейся на пиринговом программном обеспечении нового поколения.

Ранее уже предпринималось несколько попыток организации передачи голоса через интернет в реальном времени, как на основе уже существующих технологий – ICQ, AIM, так и с разработкой новых способов, например, так

---

[147] DDoS – Distributed Denial Of Service, распределенная атака на отказ в обслуживании. При проведении DDoS-атаки открывается максимально возможное количество соединений на тот или иной сервис, либо посылается большое количество определенного типа пакетов. Если операционная система не успевает обработать все пакеты, происходит переполнение буфера, и компьютер перегружается или виснет.

Отказ в обслуживании (DoS) является типовой атакой и достаточно подробно исследован. Сущность DoS-атаки заключается в том, чтобы лишить пользователей какого-либо сервиса или службы возможности обратиться к этому сервису. Технически это можно осуществить несколькими способами: путем перегрузки сети за счет передачи «мусора» и другого паразитного трафика, препятствуя тем самым передаче законного сетевого трафика; путем прямого разрушения связи между двумя машинами, таким образом предотвращается доступ к службе; путем лишения доступа к службе конкретного пользователя (как правило, за счет лишения этого пользователя привилегий доступа); путем прямого выведения сервиса из строя (когда сам сервис полностью доступен, но выполнять свои функции он не может); и т. д.

В основе распределенной DoS-атаки лежит установка огромного количества серверов DDoS на различных компьютерах, ожидающих команды от центрального клиента. В определенный момент времени центральный клиент посылает на все серверы сообщение, содержащее инструкцию о начале атаки одного адресата. Центральный клиент распределяет работу по посылке пакетов адресату среди всех доступных серверов DoS, поэтому DDoS и называется распределенной атакой.

[148] «Троянские кони» (трояны, троянцы) – самый опасный тип компьютерных вирусов, которые позволяют удаленно контролировать зараженный компьютер. Таким образом, виртуальный злоумышленник может произвести любые действия с компьютером жертвы: удалять, копировать, создавать, загружать файлы, запускать любые приложения, управлять аппаратными устройствами компьютера.

называемая технология VoIP[149]. На VoIP, в частности, базируются службы IP-телефонии. Однако из всех попыток ни одна, кроме, пожалуй, IP-телефонии, не оказалась достаточно успешной.

Выход Skype стал в этом плане знаменательным. Слияние современных технологий сжатия, кодирования, хранения и передачи данных позволило создать продукт, способный полностью заменить телефон при общении, при этом расстояние становится несущественным, разговор с абонентом на другом континенте стоит для пользователя столько же, сколько и с соседом по подъезду.

Успеху способствовали несколько аспектов.

Во-первых, чрезвычайно удачный аудиокодек[150]. Если предшествующие программы давали качество звука, заметно уступающее обычному телефону, то кодек, применяемый в Skype, дает звук высокого качества. Кроме того, он очень экономен и хорошо приспособлен под интернет.

Вторая причина успеха – тщательно проработанный интерфейс и его высокая дружественность к пользователю. Интерфейс Skype очень напоминает ICQ, с учетом, естественно, специфики программы. Удобство же ICQ было далеко не последним фактором ее успеха. Авторизация и отслеживание участников системы осуществляются на сервере компании централизованно, а вот голосовой трафик идет от пользователя к пользователю напрямую.

Третья причина – высокая устойчивость связи, даже при использовании каналов не очень высокого качества.

2.10.9. Глобальные сети распределенных вычислений

Под термином «распределенные вычисления»[151] понимается использование множества соединенных в сеть компьютеров для проведения вычислительных операций, требующих колоссальных мощностей. Совокупная мощь развитой сети распределенных вычислений может значительно превышать производительность самых мощных суперкомпьютеров мира.

---

[149] Voice over IP.

[150] Аудиокодек – кодер-декодер аудиоинформации. Кодер – программа для сжатия цифрового потока, содержащего аудиоданные, за счет исключения части звукового спектра, а также некоторого статистического анализа. Декодер выполняет обратную задачу и восстанавливает исходный сигнал – за вычетом, разумеется, исключенной части спектра.

[151] Также применяется термин «Grid Computing», предложенный Иеном Фостером, одним из исследователей, работающих в области распределенных вычислений.

Идея выполнять сложные расчетные задачи с помощью сразу нескольких процессоров родилась давно. Кластерные вычисления с использованием архитектур MPI[152] или PVM[153] возможны уже много лет. Первый Beowulf-кластер был построен почти 10 лет назад в NASA, после чего этот способ создания недорогих но высокопроизводительных систем начал широко использоваться в области академических исследований. Но, хотя Beowulf-кластеры и дешевы настолько, что их себе могут позволить большинство исследовательских лабораторий, они ограничены в размерах доступным пространством, а также предполагают значительные затраты на электроснабжение и охлаждение.

Распределенные вычисления обходятся намного дешевле. Исследователям больше не нужно самим покупать компьютеры: вычислительные ресурсы предоставляются пользователями по всему миру. Благодаря быстрому распространению интернета появилась возможность объединить огромный объем вычислительных ресурсов в одну систему.

На сегодняшний день распределенные вычисления являются важной составляющей научных и технологических исследований, а также оказывают немалое влияние на развитие интернета. Ниже перечислены наиболее крупные из существующих сетей распределенных вычислений и их основные задачи.

Distributed.net

Первым проектом распределенных вычислений, получившим широкую известность, был Distributed.net. Еще в самом начале 1997 года группа энтузиастов занялась проверкой устойчивости 56-битного алгоритма шифрования RC5-32/12/7[154] компании RSA Labs[155]. Первому из участников, кому удастся

---

[152] MPI – Message passing interface, интерфейс передачи сообщений. Стандартизованный механизм для построения параллельных программ в модели передачи мультикомпьютерных и кластерных сообщений. Введен Форумом по интерфейсу передачи сообщений в апреле 1994 г. В настоящее время MPI – наиболее широко используемый и динамично развивающийся интерфейс из своего класса.

[153] PVM – Parallel virtual machine, параллельная виртуальная машина – программный пакет, позволяющий объединить сетью разнородную совокупность Unix-компьютеров и использовать их как единый большой параллельный компьютер. PVM очень легко переносится, его исходные коды могут быть откомпилированы в программу на любом компьютере от ноутбука до CRAY.

[154] RC5 – Rivest's cipher 5, блочный шифр, разработанный Роном Ривестом из компании RSA Security Inc. Алгоритм RC5 имеет переменные длину блока, количество раундов и длину ключа. Для спецификации алгоритма с конкретными параметрами принято обозначение RC5-W/R/K, где W равно половине длины блока в битах, R – число раундов, K – длина ключа в байтах.

это сделать был обещан денежный приз. Таким образом, у пользователей появлялся шанс заработать, всего лишь предоставляя неиспользуемое вычислительное время своего компьютера. Всего в Distributed.net принимало участие более 300000 пользователей. Уже 22 октября 1997 года код для расшифровки сообщения был подобран компьютером, а всего расшифровка ключа заняла 212 дней работы. Характерно, что при старте проекта расчетное время подбора кода составляло несколько десятков лет. Однако быстрый рост количества участников проекта позволил значительно сократить этот период. В конце соревнования в проекте насчитывалось более 26 тысяч компьютеров, подключенных к расчетам, а энтузиасты объединились в команды числом более 4000. Подбор кода спонсировался компанией RSA Labs с целью демонстрации устойчивости ключа. Действительно, только объединение таких вычислительных мощностей позволило разгадать код в какие-то разумные сроки (скорость перебора на момент завершения проекта превысила 7 миллиардов ключей в секунду).

Таким образом, шифр с самыми слабыми параметрами RC5-32/12/5 был взломан в течение нескольких часов. На взлом шифра RC5-32/12/7 было затрачено более полугода. Последний осуществленный взлом шифра RC5-32/12/8 потребовал 5 лет. Неприступными пока остаются RC5-32/12/K для K=9…16. В настоящее время ведется проект RC5-72 для взлома RC5-32/12/9.

27 октября 1997 года был создан и одобрен устав компании Distributed.net. После проекта RC5 Distributed.net принимала участие еще в целом ряде проектов.

- DES-II-1 – конкурс с ограничением времени, организован RSA Labs, проходил 13.01.1998-24.02.1998;
- DES-II-2 (он же DES-III), конкурс с ограничением времени, проходил 13-14 марта 1999 года. В этом конкурсе Distributed.net не смогла обогнать Electronic frontier foundation, расшифровавшую текст «It's time for those 128-, 192-, and 256-bit keys» аппаратными средствами.

---

[155] RSA – асимметричная система с открытым ключом (public-key) предназначенная как для шифрования, так и для аутентификации. Разработана в 1977 году математиками Ривестом, Шамиром и Эльдерманом (Rivest, Shamir и Alderman). Она основана на трудности разложения очень больших целых чисел на простые сомножители. После создания программы, реализующей криптографический алгоритм шифрования на основе RSA, была зарегистрирована компания RSA Labs, занимающаяся продвижением продукта на рынке.

GENOME@home Classic

GENOME@home («Геном дома») – проект, направленный на решение задачи расшифровки генома человека. Проводился в 2001-2003 гг. Стенфордским университетом (Калифорния, США) и завершился успехом.

Задачей проекта было сравнение известных генетических данных со строением белковых молекул, что должно позволить найти кодирующие их (молекулы) генетические последовательности, а затем искусственно синтезировать белки.

ECC2-109

Цель проекта заключалась во взломе криптографического алгоритма ECC2-109. Проект занимался вычислением так называемых «разделенных точек», пытаясь найти коллизию между ними.

Каждый раз, когда компьютер участника обнаруживал разделенную точку, он отправлял ее на центральный сервер (либо, при отсутствии доступа к Интернету, сохранял в буфере для последующей отправки).

Затем центральный сервер проверял, не совпадает ли эта точка с другой, найденной кем-то еще. Такое совпадение и называлось коллизией. При обнаружении коллизии в апреле 2004 года проект завершился.

RSAttack 576

Проект RSAttack 576 занимался взломом криптографического ключа в рамках конкурса, проводимого RSA Security. Клиентская часть RSAttack занималась факторизацией 576-битного числа. Работа проводилась по обычной схеме: клиент скачивал с сервера пакеты заданий, обрабатывал их и отсылал результат.

Ключ RSA-576 был факторизован в декабре 2003 года. В настоящее время проект RSAttack сейчас приостановлен, идет подготовка к запуску RSAttack 640.

ZetaGrid

ZetaGrid – распределенная вычислительная система с открытыми исходными кодами, использующая свободные ресурсы подключенных к ней компьютеров. Она может быть использована для любого вычислительно-емкого приложения, которое разделяется на множество отдельных шагов,

причем каждый из них может выполняться на отдельном компьютере достаточно продолжительное время.

Лаборатория IBM в г. Боблинген (Германия) использует ZetaGrid для проверки гипотезы Римана – одной из важнейших задач современной математики. В проекте участвуют более 5000 компьютеров, пиковая производительность достигает более чем 5600 гигафлоп. Каждый день проект обнаруживает примерно один миллиард нулей zeta-функции.

В конце 2004 года проект достиг цели – 1 миллиарда проверенных нулей зета-функции. В январе 2005 он был приостановлен. За это время удалось создать не только мощную и масштабируемую платформу для распределенных приложений, но и заметно продвинуть теорию чисел в области исследования гипотезы Римана.

Lifemapper

Проект Lifemapper занимался составлением электронного атласа биологического разнообразия Земли. Интернет использовался для получения из национальных исторических музеев информации о растениях и животных. Участники проекта анализировали эти данные, конструировали экологический профиль для каждого из видов, составляли карты их местонахождения и предсказывали, где они потенциально могли бы жить.

Результаты могут помочь в биологических исследованиях, образовании, сохранении живой природы по всему миру, а также в предсказании различных экологических событий и катаклизмов.

Распределенная часть проекта завершена в декабре 2004 года.

Distributed Folding

Проект занимается моделированием белков. В ходе проекта предполагается получить данные, важные для понимания причин многих болезней.

Особенность проекта в следующем: в нем сервер как таковые задания не распределяет, только принимает результаты. Клиент на основе заложенных в него данных об атомах и их возможных соединениях создает случайные протеины, которые потом и отправляет на сервер.

Проект приостановлен с октября 2004 года.

MD@home

Проект занимается изучением особенностей поведения фрагментов белковых цепочек (олигопептидов). Цель исследования – изучить взаимовлияние аминокислот друг на друга в зависимости от положения в олигопептидах. Если его удастся закончить, возможен серьезный прорыв в понимании принципов конструирования белков.

В августе 2003 года проект приостановлен на неопределенный срок.

SETI@home

Программа SETI[156] основывается на предположении, что систематический поиск в космосе может выявить искусственные сигналы, испускаемые либо намеренно, либо в качестве случайного электромагнитного шума, подобно тому, как Земля испускает целый диапазон ТВ и радиосигналов.

Начиная с 1992 года радиотелескоп Arecibo[157] целенаправленно обшаривает небесный свод в поисках посланий от инопланетян. Объем поступающей с телескопа информации колоссален, а расчеты, выполняемые для спектрального анализа сигнала, оказываются очень трудоемкими. Обработка информации потребовала бы использования крайне дорогостоящего компьютера очень высокой производительности.

Выход был найден в методике распределенных вычислений в интернете. Метод распределенных вычислений мобилизует возможности миллионов персональных компьютеров, подключенных во всем мире к сети интернет. Информация, подлежащая численной обработке, разбивается на относительно небольшие блоки. Пользователь, желающий принять участие в программе распределенных вычислений, устанавливает на своем компьютере специаль-

[156] SETI – Search for extraterrestrial intelligence, поиск внеземного разума.

[157] Радиотелескоп в Аресибо (Пуэрто Рико) – один из крупнейших радиотелескопов на Земле. Основное зеркало телескопа сферическое, имеет диаметр 305 м. Изначально радиотелескоп создавался как локатор для исследования верхней ионосферы Земли. Но ввиду большой площади, обеспечивающей исключительно высокую чувствительность, он оказался исключительно подходящим для целей радиоастрономии. Телескоп может работать в диапазоне длин волн от 6 м до 3 см. На нем ведутся программы наблюдений в спектральных радиолиниях на волнах 21 см (линия нейтрального водорода), 18 см (линии гидроксила OH), в непрерывном спектре на метровых волнах (поиск и исследование пульсаров) и др. С 1992 г. в рамках проекта SERENDIP им выполняется поиск внеземных цивилизаций на волне 21 см. Телескоп также используется как передающая антенна для радиолокации планет, мощность передатчика 1 МВт.

ную программу, которая работает как скринсейвер[158]. Если компьютер некоторое время не занят работой, программа активируется, загружает через интернет с центрального сервера проекта блок информации и осуществляет его обработку, после чего результат отсылается на центральный сервер. Во время работы программы на экране монитора отображается красивая движущаяся картинка, показывающая, что программа активна.

На ноябрь 2004 года во всем мире программа SETI@home была установлена более чем на 5 миллионах персональных компьютеров в 226 странах, всего на обработку данных из Аресибо было уже затрачено 2 млн. лет компьютерного времени – гораздо больше, чем смог бы сделать самый мощный из существующих суперкомпьютеров.

Climate Prediction

Результатом проекта должен стать общий прогноз погоды на 50 лет вперед. Основная цель – определить, насколько точны существующие методы долговременного предсказания погоды, и насколько сильно на их точность влияют погрешности в исходных данных.

Проект совместно проводят университеты Оксфорда и Рединга, Метеорологический центр Великобритании, Рутерфорд-Аплтонская лаборатория и софтверная компания Tessella Support Services.

DataGRID

DataGRID – высокоскоростная вычислительная сеть на базе ОС Linux, распределенная по всей Европе. Предполагается, что после запуска сеть станет главным вычислительным ресурсом Европы.

Концепция распределенной вычислительной сети GRID была сформулирована в 1999 году учеными CERN[159]. Конкретной реализацией этой кон-

---

[158] Скринсейвер – транскрибированное английское «screensaver», букв. «хранитель экрана», специальная программа, включающаяся после некоторого времени простоя компьютера. Гасит изображение на экране или заменяет его абстрактными неподвижными или движущимися изображениями. Прежде они предотвращали таким образом преждевременное выгорание люминофора в кинескопах мониторов, а к настоящему времени превратились в вид неочевидного искусства и самовыражения.

[159] CERN (ЦЕРН) – Европейский центр ядерных исследований, крупнейшая в мире лаборатория физики высоких энергий. Аббревиатура CERN произошла от французского Conseil européen pour la recherche nucléaire (букв. Европейский совет по ядерным исследованиям). CERN находится на границе Швейцарии и Франции, вблизи Женевы. Основан 29 сентября 1954 года. Первоначально его членами числилось 12 европейских стран, позже

цепции стал открытый проект DataGRID. Его поддержали многие частные и общественные организации, координировал развитие CERN, а финансировал – Евросоюз.

Изначально DataGRID предназначалась для обработки данных Большого адронного коллайдера[160] – самого мощного на сегодняшний день ускорителя частиц, который построил CERN. Строительство коллайдера завершено в 2006 году, к середине 2007 планируется его запуск.

Поток данных для обработки будет колоссальным – несколько миллионов гигабайт в год. Это потребует вычислительную среду в тысячи раз более мощную, чем может обеспечить даже современный Интернет. Никакая SETI-подобная интернет-система распределенных вычислений с таким объемом информации не справится. Концепция GRID предусматривает обмен данными в реальном времени по скоростным линиям. Предполагается, что мощность DataGRID превысит 15 трлн. операций в секунду (15 терафлоп), что на порядки больше любого существующего ныне суперкомпьютера.

К моменту запуска коллайдера вычислительная сеть уже должна будет работать. Пользоваться ею смогут не только физики, но и другие ученые и организации.

Прочие распределенные вычислительные сети

- *Einstein@home* – анализ данных детекторов гравитационных волн, расположенных в США и Германии, для поиска гравитационных сигналов от быстро вращающихся нейтронных звезд;
- *LHC@home* – моделирование процессов, которые будут происходить

их число возросло до 20. В CERN постоянно работают около 3000 человек, также около 6500 физиков и инженеров из 500 университетов и институтов всего мира участвуют в экспериментах.

Основное направление деятельности – изучение структуры материи и фундаментальных сил природы, но вообще тематика исследований весьма широка. В частности, именно в ЦЕРНе в 1989 году ученый Тим Бернерс-Ли, бывший в то время сотрудником лаборатории, разработал концепцию и приступил к созданию информационной службы World Wide Web.

[160] LHC – Large hadron collider, Большой адронный коллайдер. Ускоритель элементарных частиц, представляющий собой расположенное на глубине 120 метров под землей кольцо идеальной формы диаметром 27 километров. В коллайдере планируется разгонять элементарные частицы до скоростей, близких к световым, и изучать эффекты, возникающие при их столкновении. Одной из первых задач, которые предполагается решить на коллайдере, является выяснение природы массы. Результаты могут существенно изменить представления ученых о физической картине Вселенной.

в Большом адронном коллайдере CERN; проект направлен на усовершенствование конструкции ускорителя частиц;

- *Find-a-drug* – разработка средств противодействия биотерроризму, поиск лекарств от рака, СПИДа и атипичной пневмонии, а также создание безопасных гербицидов;
- *Folding@home* – получение более точного представления о болезнях, вызываемых дефектными белками, причем в основном изучаются белки, имеющие отношение к болезни Альцгеймера, Паркинсона, диабету типа II, коровьему бешенству и склерозу;
- *grid.org Cancer Research Project* – моделирование взаимодействия миллиардов возможных молекул с протеинами, участвующими в развитии раковых заболеваний; цель проекта заключается в определении, не является ли одна из этих молекул возможной основой для нового лекарственного средства;
- *Predictor@home* – исследование заболеваний, связанных с нарушением структуры белка;
- *Fermat Search* – проект, проводимый российскими учеными, направленный на поиск новых делителей для чисел Ферма;
- *Great Internet Mersenne Prime Search (GIMPS)* – поиск новых простых чисел Мерсенна[161]; самое большое известное на данный момент простое число $M_{20996011} = 2^{20996011}-1$ было найдено в рамках проекта GIMPS в ноябре 2003 года, всего таких чисел известно 40;
- *Number Field Sieve Network (NFSNET)* – проект факторизации[162] больших чисел с помощью метода «Number Field Sieve»[163];
- *MoneyBee* – анализом биржевых котировок и индексов, а также предсказание их будущих изменений с помощью технологии нейронных сетей;

---

[161] Числа Мерсенна – особый вид простых чисел вида 2^p-1 , где p – простое число. Названы по имени французского монаха Мерсенна (1588-1648), одного из основателей Парижской Академии наук, друга Декарта и Ферма. Впервые же о числах такого характера упоминал еще Евклид в 350 году до н.э. С тех пор они являются одной из центральных тем раздела математики под названием теория чисел.

[162] Факторизация – разложение на простые множители.

[163] Number field sieve (NFS) – самый быстрый в настоящее время алгоритм факторизации больших составных целых общего вида. Разработан Дж. М. Поллардом в 1988 году, в дальнейшем усовершенствован несколькими известными в области теории чисел учеными.

• *The World Community Grid* – проект, спонсируемый корпорацией IBM, разработавшей программное обеспечение, позволяющее быстро и с минимальными затратами строить глобальные распределенные суперкомпьютеры, отдельные части которого будут связаны между собой через интернет. О его создании объявлено в конце 2004 года. В перспективе эта сеть должна стать одной из самых крупных не только по совокупной вычислительной мощности подключенных пользовательских машин, но и по их количеству: программное обеспечение IBM позволяет строить распределенные суперкомпьютеры, состоящие из десяти и более миллионов звеньев.

2.11. America OnLine

America OnLine не является фирмой, представляющей сугубо информационные технологии. Однако роль корпорации в развитии интернета и различных его сервисов настолько велика, а судьба настолько интересна и неоднозначна, что имеет смысл немного подробнее изложить здесь историю ее развития.

Корпорация AOL – America OnLine основана в 1985 году. Первоначальное название – Quantum Computer Services, основная деятельность – предоставление различных платных онлайновых сервисов. В 1987 году фирма сменила название на America OnLine.

По большому счету, история AOL – это история слияний, поглощений и покупок других фирм, как более мелких, так и более крупных. Первое крупное слияние произошло с компанией CompuServe (1,2 млрд. долларов), за счет чего AOL смогла расширить свое влияние на европейский рынок (CompuServe насчитывала около пяти миллионов постоянных пользователей в 80 странах мира). В декабре 1998 года AOL купила компанию Netscape Communications (4,2 млрд. долларов). В результате, помимо браузера Netscape, во владение к AOL перешел также сайт Netcenter, у которого на тот момент насчитывалось около 20 млн. пользователей. Вскоре после этого компании AOL и Sun Microsystems объявили о долгосрочном сотрудничестве в разработке технологий Java. В 1999 году AOL купила компанию Nullsoft, а в 1998 году – Mirabilis, основного конкурента в IM-сетях.

В 2001 году произошло объединение корпораций AOL и Time Warner. Интересным было то, что медиа-империя Time Warner была в пять раз больше, чем компания AOL, однако владельцу AOL Стиву Кейсу удалось добить-

ся доминирующего положения в объединенной компании. Образно выражаясь, селедка проглотила кита. Произошло все очень просто. Стив Кейс в начале 2001 года просто позвонил главе руководства Time Warner Джеральду Левину и популярно объяснил тому, что к передовым информационным технологиям, которые предоставляет AOL, просто-таки необходимо добавить информационную составляющую, которую обеспечит Time Warner. С этого момента берет начало история корпорации AOL Time Warner, капитализация которой была оценена более чем в 250 млрд. долларов.

Структура AOL Time Warner достаточно сложна. Это пестрый конгломерат из множества маленьких и больших компаний, которые, сливаясь воедино, образуют огромную медиаимперию. Ниже перечислены наиболее крупные и доходные подразделения AOL Time Warner, ставшие таковыми благодаря умелому совмещению компьютерных и телекоммуникационных технологий с традиционными средствами массовой информации.

1). *Интернет-портал AOL*. В 80-90-х годах XX века у большинства пользователей интернет в США ассоциировался исключительно с онлайновыми сервисами AOL. После появления WWW сайт компании AOL долгое время был самым посещаемым. Всякий пользующийся интернетом американец считал своим долгом иметь почтовый ящик на www.aol.com (тем более что других на тот момент практически не существовало). Компания AOL предоставила пользователям сети то, в чем они нуждались, – огромный портал, на котором можно было найти все, начиная с игр и заканчивая форумами различной тематики.

2). *Подразделение интерактивных сервисов America OnLine*. Образована в 1985 году, с тех пор достигла значительных успехов в областях интернет-технологий, интерактивных сервисов и электронной коммерции. Среди успехов подразделения такие программные продукты, как AOL Instant Messenger, AOLbyPHONE, AOL@School; концепции Digital City, AOL Anywhere.com, iPlanet E-Commerce Solutions, NullSoft Winamp, Mirabilis ICQ, браузеры Netscape Navigator и Communicator и другие разработки.

- *AOLbyPHONE* – сервис, позволяющий получать по телефону заказанную заранее информацию, которая будет продиктована синтезированным голосом;
- *AOL@School* – проект, предназначенный для обучения школьников, содержит сертифицированные специалистами материалы, облегчающие ус-

воение школьной программы, а также огромное количество ссылок на дополнительную информацию в Интернете;

- *Digital City* – проект виртуального города со всеми его преимуществами и недостатками: это и организация виртуального рынка, и создание виртуальных универмагов и магазинов, центров развлечений, отдельных офисов, а также виртуальной полиции, обеспечивающей порядок;
- *AOL Anywhere.com* – сервис, позволяющий доступ с любого устройства (PDA, мобильный телефон, пейджер и др.) к сервисам и контенту, предоставляемому AOL;
- *iPlanet E-Commerce Solutions* – проект, разрабатываемый совместно с Sun Microsystems[164], включает программное обеспечение и некоторые сервисы для организации и доступа к виртуальным офисам, магазинам и другим платформам е-коммерции;

3). *Turner Broadcasting* – телевизионное подразделение, занимается главным образом подготовкой новостей, телепередач и другого контента. Основной канал распространения – Home Box Office, одна из крупнейших в США сетей домашнего телевидения, насчитывает около 50 миллионов подписчиков. Также активно развивается AOL Time Warner Interactive Video – подразделение интерактивного видео, которое должно сменить Home Box Office.

4). *Time Warner Trade Publishing* – одно из самых молодых подразделений компании, занимается изданием книг различной тематики, количество наименований выпускаемых издательством книг увеличивается ежемесячно на 50 штук.

5). *Warner Bros.* – старейшее и одно из самых прибыльных подразделений AOL Time Warner, создана в 1918 году братьями Уорнер в Калифорнии. На сегодняшний день Warner Bros. – лидер мировой киноиндустрии. Также в

[164] Sun Microsystems – одна из крупнейших компьютерных корпораций США, производящая программное и аппаратное обеспечение. Основана в 1982 году. SUN – аббревиатура от Stanford University Networks. Традиционно является одним из крупнейших производителей серверов и рабочих станций на базе собственных процессоров SPARC и процессоров Opteron компании AMD. Разрабатывает собственную операционную систему Unix-подобного типа, называющуюся Solaris. Крупным вкладом Sun в развитие современных информационных технологий стало создание платформы Java. Кроме того, с 1999 г. Sun выпускает StarOffice – комплексный пакет офисного ПО, включающий текстовый, табличный и графический редакторы, программу подготовки презентаций и настольную СУБД. На основе открытых и опубликованных исходных текстов StarOffice благодаря усилиям энтузиастов возник проект OpenOffice.org, сам офисный пакет на основе опубликованных исходных текстов был также назван OpenOffice.org и распространяется бесплатно.

эту структурную нишу входит New Line Cinema – одна из самых именитых киностудий Голливуда.

6). *Warner Music Group* – один из крупнейших мировых издателей музыки.

Контрольные вопросы к разделу

1. Расскажите хронологию становления сети ARPANET. Выделите основные моменты развития сети и базовых принципов, легших в ее основу. Объясните, как и почему ARPANET, которой прочили незавидное будущее, превратилась в интернет.
2. Приведите примеры глобальных сетей, опишите технологии, характерные отличия и особенности. Какие из этих сетей возникли спонтанно, и что явилось этому причиной?
3. Перечислите основные службы интернета. Каковы их особенности, достоинства и недостатки?
4. Что представляет собой технология P2P? Какие направления развития пиринговых сетей вы можете назвать? В чем их особенности и недостатки в техническом и правовом планах?
5. Объясните причины успеха служб мгновенных сообщений. Как вы думаете, насколько сильно влияние сервиса IM на современное делопроизводство? Как ситуация будет изменяться со временем?
6. Что обусловило появление файлообменных сетей? Как повлияло распространение таких сетей на развитие интернета? Проследите изменение характера данных, передаваемых по сети, с начала 90-х годов прошлого века до настоящего времени.
7. Чем обусловлена востребованность сетей распределенных вычислений? Что это за сети, на каких технологиях они основаны? Для каких целей они сегодня используются? Приведите примеры самих сетей и проектов, решаемых и решенных с их помощью.
8. Каким вы видите будущее интернета?

3. НЕКОТОРЫЕ АСПЕКТЫ ЗАКОННОСТИ И БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В МИРОВЫХ СЕТЯХ

3.1. Понятие защиты информации

Защита информации – понятие достаточно сложное. В информационной сфере оно подразумевает два таких достаточно разных направления, как защита от утраты (повреждения) и защита от утечки. Поскольку причины того и другого различны, методы и подходы к обеспечению защиты информации по этим направлениям также различаются.

Рассматривая защиту информации от утраты, следует иметь в виду что автоматизированные системы, обрабатывающие информацию, являются сложными техническими системами. Недостаточная надежность функционирования таких систем, сбои и отказы в работе тех или иных функциональных устройств могут привести к потере информации. В ряде случаев стоимость обрабатываемой информации значительно превосходит стоимость оборудования, входящего в состав системы. В таких ситуациях ставится задача сохранения информации даже в условиях производственных катастроф и стихийных бедствий. Рассмотрение методов защиты информации от повреждения выходит за рамки данного учебного пособия. Интересующимся можно порекомендовать обратиться к соответствующей литературе.

С компьютерными сетями тесно связан другой аспект защиты – от утечки. Как правило, утечка происходит не по собственной воле информационного массива, а по злому умыслу заинтересованного лица (лиц). Чтобы сформулировать задачи защиты информации от злоумышленников, необходимо представить себе их цели и возможности по достижению этих целей.

Обычно различают следующие цели нарушителя:

- незаконное завладение конфиденциальной информацией;
- модификация информации;
- уничтожение информации;
- нарушение функционирования автоматизированной системы;
- незаконное копирование программ (и другой ценной информации);
- отказ от информации.

Под *конфиденциальной информацией* будем понимать информацию, доступ к которой ограничен в соответствии с законодательством. Факт попа-

дания такой информации злоумышленнику называют *утечкой информации*. Утечка информации может быть разной по последствиям. Так, например, утечка информации, связанная с хищением носителя или даже компьютера в целом, очень быстро обнаруживается. В то же время негласная для законного владельца утечка информации наносит больший вред.

Модификация информации всегда подразумевается неявной для законного владельца информации. Модификация информации может проявляться по разному. Например, в финансовом документе она может заключаться в «исправлении» номера счета, куда надо переслать деньги, или размера суммы, подлежащей перечислению по указанному адресу. В сетях с коммутацией пакетов модификация может заключаться в изъятии из канала связи части сообщения, изменении порядка следования частей сообщения. Наконец, возможен повтор или посылка фальсифицированного сообщения, например, с указанием банку перечислить деньги.

Уничтожение информации может привести к краху вычислительной системы, если не были приняты профилактические меры по резервному копированию информации, и к временному выходу системы из строя при наличии резервных копий.

Под *нарушением функционирования* автоматизированной системы подразумевают (в отличие от уничтожения информации) скрытные действия, мешающие нормально функционировать системе. Такие действия могут осуществляться захватом ресурсов, запуском на решение посторонних задач или повышением приоритетности задач, не требующих срочного решения. К таким вмешательствам в работу наиболее чувствительны информационные системы, работающие в режиме реального времени или в режиме оперативного принятия решений.

Говоря о *незаконном копировании программ*, имеют в виду копирование не конфиденциальной информации, а информации, распространяемой на коммерческой или другой договорной основе. Незаконное копирование программ и другой ценной информации рассматривается как нарушение авторских прав разработчиков программного продукта и баз данных.

При рассмотрении целей злоумышленника необходимо отметить следующее обстоятельство. При создании той или иной системы защиты информации в автоматизированной системе или сети, злоумышленник лишается возможности достичь своих целей наиболее простыми и доступными (как

в отсутствие защиты) средствами. В новых условиях злоумышленник постарается исследовать внедренную систему защиты и найти пути ее преодоления. При этом у него появляются новые цели: узнать ключи или пароли, модифицировать программное обеспечение системы защиты информации и тем самым полностью или частично нейтрализовать защитный механизм, обойти его. Такие цели носят по сравнению со сформулированными выше промежуточный характер. Но эти цели обязательно учитываются при проектировании и внедрении средств защиты информации.

Нематериальный характер информации затрудняет решение проблем по ее защите. В самом деле, рассмотрим пример: некто завладел информацией, скопировав без разрешения файл с магнитного носителя. При этом информация как была в распоряжении хозяина, так и осталась. Даже размер носителя нисколько не изменился. В этих условиях трудно признать кражей факт копирования информации, если понимать кражу традиционно, как изъятие вещи у владельца. Без законодательной поддержки, учитывающей особую природу информации, невозможно организовать ее защиту. Законодательство по вопросам информации и информатизации по необходимости является первым звеном в системе защиты информации.

Основу законодательства Российской Федерации по защите информации в настоящее время составляют следующие законы:

- Федеральный закон «Об информации, информатизации и защите информации», принятый Государственной думой 25 января 1995 года;
- Закон Российской Федерации «О государственной тайне» принятый Верховным Советом Российской Федерации в 1993 году и вступивший в полную силу с 1 января 1995 года;
- Закон Российской Федерации «О правовой охране программ для ЭВМ и баз данных», принятый Верховным Советом Российской Федерации 23 сентября 1992 года;
- часть 4 Гражданского кодекса Российской Федерации «Права на результаты интеллектуальной деятельности и средства индивидуализации», принятая в январе 2007 года.

Кроме того, в принятом в 1996 году и введенном в действие с 1 января 1997 года новом Уголовном кодексе Российской Федерации впервые предусмотрена уголовная ответственность за ряд компьютерных преступлений.

Находится в разработке Закон Российской Федерации «О коммерческой тайне».

В Федеральном законе «Об информации, информатизации и защите информации» определен правовой статус информации. Признано, что информация может быть ресурсом и товаром, определено разделение информации на общедоступную и информацию ограниченного доступа. В соответствии с законом, целями защиты информации и прав субъектов в области информатизационных процессов и информатизации являются:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз информационной безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, секретности, конфиденциальности документированной информации в соответствии с действующими законодательными актами;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, информационных технологий и средств их обеспечения.

3.2. Направления защиты информации

Перечисляя уязвимые места автоматизированных систем и сетей с точки зрения защиты информации, необходимо перечислить элементы, их составляющие.

1. Рассмотрим отдельную автоматизированную систему, представляющую собой компьютер или локально-вычислительную сеть. Иногда для краткости будем называть ее просто системой.

Если злоумышленник получил доступ к компьютеру с защищаемой информацией, то он может ее скопировать, изменить или уничтожить. Кроме того, нарушитель может вывести компьютер из строя или предпринять действия по нарушению функционирования автоматизированной системы, элементом которой тот является.

При наличии в автоматизированной системе ограниченного доступа для ее защиты обычно формулируются и реализуются правила разграничения доступа. В соответствии с Федеральным законом «Об информации, информатизации и защите информации», защите должна подлежать любая информация, входящая в состав информационного ресурса или являющаяся собственностью либо товаром. Поэтому правила разграничения доступа должны быть сформулированы всегда. Их минимальным содержанием должно быть различение пользователей по принципу «свой–чужой». Действия злоумышленника по получению доступа к информации в обход правил разграничения доступа (с использованием только штатных средств вычислительной системы) называются *несанкционированным доступом*.

2. Компьютер и его составные части: системный блок, дисплей, клавиатура – являются элементами электронного оборудования. Происходящие в них физические процессы во время функционирования, приводят к возникновению переменных электромагнитных полей. Указанные поля могут нести в себе защищаемую информацию ограниченного доступа. Эта информация может улавливаться специальными приемными устройствами на некотором удалении от компьютера. В данном случае говорят об *уязвимости от паразитных электромагнитных излучений*.

При определенных условиях утечка информации может быть организована по акустическому, оптическому, вибрационному каналам. В общем случае говорят об *уязвимости к утечке информации по техническим каналам утечки*.

3. Рассмотрим теперь автоматизированную систему в составе телекоммуникационной сети. Даже если она защищена от несанкционированного доступа к информации, она уязвима от злоумышленника, имеющего удаленный доступ. Более того, удаленный доступ может принести больший вред, чем несанкционированный доступ внутри системы. Дело в том, что в рассматриваемом случае злоумышленник может потратить на исследование возможности проникновения в систему значительное время и остаться при

этом анонимным. В результате проникновения он может достичь тех же целей, что и при несанкционированном локальном доступе: утечки, искажения и/или уничтожения информации. Он может попытаться нарушить функционирование системы запустив решение своей, быть может бессмысленной задачи, требующей всех или почти всех ресурсов системы. Другими способами нарушения функционирования системы могут быть организация потока запросов, критичного по объему для системы, либо запуск вируса или червя.

4. Весьма уязвимы сети в случае получения злоумышленником доступа к узлу связи, а также при подключении к коммутационному оборудованию. В этих случаях злоумышленник получает возможность:

- считывать и модифицировать информацию, проходящую через точку подключения;
- блокировать прохождение информации;
- записывать и посылать сообщения повторно;
- создавать и посылать свои сообщения, маскируя их под сообщения законных пользователей;
- наблюдать трафик (интенсивность и объемы обмена информацией, направления передачи информации).

5. Примерно такие же возможности имеются у злоумышленника, подключившегося к каналу связи. Однако сама такая возможность подключения зависит от физической природы канала. Наиболее чувствительны к перехвату информации радиоканалы и, в том числе, каналы спутниковой связи. Подключение к каналу связи в этом случае производится с использованием антенны и соответствующего связного оборудования. Подключение остается практически незаметным для законных пользователей сети.

Кабели, используемые при передаче информации, могут быть трех типов:

- витая пара;
- коаксиальный кабель;
- оптоволоконный кабель.

Подключение к кабелю типа *витая пара* осуществляется с помощью непосредственного электрического контакта, либо с использованием индуктивной или емкостной развязки. Подключение к коаксиальному кабелю более трудное, но и его стоимость выше.

Оптоволоконный кабель представляет собой световод в защитной оболочке, информация передается с помощью модулированного электромагнит-

ного излучения в диапазоне волн видимого света. Информация может передаваться на значительные расстояния, стоимость кабеля достаточно велика. Зато незаконное подключение к такому кабелю без нарушения его работоспособности (а значит – легко обнаруживаемое) представляет большие трудности.

3.3. Виды защиты информации

С учетом изложенного в практической деятельности выделяют следующие самостоятельные направления (основные виды защиты информации):

- защита информации от несанкционированного доступа;
- защита информации от перехвата в системах связи;
- защита юридической значимости электронных документов;
- защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок;
- защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ;
- защита от несанкционированного копирования и распространения программ и ценной компьютерной информации.

Защита от несанкционированного доступа

Защита конфиденциальной и ценной информации от НСД призвана обеспечить решение одной из двух наиболее важных задач защиты имущественных прав владельцев и пользователей ЭВМ – защиту собственности, воплощенной в обрабатываемой информации, от всевозможных злоумышленных покушений, которые могут нанести существенный экономический и другой материальный и нематериальный ущерб. К ней примыкает задача защиты государственных секретов, где в качестве собственника информации выступает государство. Основной целью этого вида защиты является обеспечения конфиденциальности, целостности и доступности информации. В части технической реализации защита от НСД сводится к задаче разграничения функциональных полномочий и доступа к информации.

Существуют два принципа формулирования правил разграничения доступа: дискреционный и мандатный.

Дискреционный принцип базируется на матричных моделях. Пусть имеется некоторое множество поименованных объектов доступа (файлы, каталоги, устройства, и тому подобное) и некоторое множество субъектов доступа (поль-

зователи, их процессы). Правила разграничения доступа записываются в виде матрицы, каждый из столбцов которой соответствует одному объекту доступа, а каждая строка соответствует одному субъекту доступа. На пересечении 1-го столбца и *j-ой* строки записываются права доступа *j-го* субъекта доступа к *i-му* объекту доступа (читать, записывать, удалять, и тому подобное).

На практике системы разграничения доступа (СРД), базирующиеся на матричных моделях, реализуются обычно в виде специальных компонент универсальных ОС или СУБД, либо в виде самостоятельных программных изделий. Существенной особенностью матричных СРД для наиболее используемых универсальных ОС является принципиальная децентрализованность механизмов диспетчера доступа, что приводит к невозможности строгого выполнения требований верифицируемости, защищенности и полноты контроля указанных механизмов.

Мандатный принцип разграничения доступа основан на том, что все объекты доступа наделяются метками конфиденциальности (например по грифам секретности: «особой важности», «совершенно секретно», «секретно», «несекретно»), а для каждого субъекта доступа определяется уровень допуска (например уровень секретности документов, с которыми субъекту разрешено работать). Тогда при общении пользователя с системой чтение разрешается только по отношению к информации соответствующего уровня конфиденциальности или ниже. А запись информации разрешается только для информации соответствующего уровня конфиденциальности или выше. Такие правила обеспечивают при прохождении информации не понижение уровня ее конфиденциальности.

В наиболее ответственных случаях используются оба принципа формулирования правил разграничения доступа.

Сама процедура доступа пользователя (в соответствии с правилами разграничения доступа) происходит в три этапа: идентификация, аутентификация и авторизация.

Идентификация заключается в предъявлении пользователем системе своего идентификатора (имени) и проверке наличия в памяти системы этого имени.

Аутентификация заключается в проверке принадлежности субъекту доступа предъявленного им идентификатора (проверка подлинности). Для реализации процедуры аутентификации используется идентификатор субъекта доступа, который является либо его секретом (пароль и тому подобное),

либо является уникальным для субъекта и гарантированно не поддающимся подделке (биометрические характеристики).

Авторизация заключается в установлении прав доступа к тому или иному ресурсу в соответствии с правилами разграничения доступа.

Простейший способ защиты автоматизированной системы от удаленного доступа несанкционированных пользователей – это отказ от работы в сети, обеспечение физической защиты от всех внешних сетевых соединений. В наиболее ответственных случаях так и поступают.

Однако такая изоляция в большинстве случаев в настоящее время невозможна. Поэтому необходимо предусмотреть простые и ясные правила осуществления коммуникаций между локальными сетями различной степени защищенности, или даже, защищенной сети с незащищенной. Защищенная локальная сеть при этом представляется как бы находящейся внутри периметра, поддерживающего секретность. Внутри периметра служба контроля доступа и другие защитные механизмы определяют, кто и к какой информации допущен. В такой среде шлюзовая система[165] может отделять защищенные системы или сети от незащищенных систем или сетей извне. Незащищенная система может общаться с защищенной только через единственный канал связи, контролируемый защищенным шлюзом. Шлюз контролирует трафик как извне, так и наружу, и эффективно изолирует защищенную сеть от внешнего мира. Благодаря тому, что брандмауэр защищает другие компьютеры, находящиеся внутри периметра, защита может быть полностью сконцентрирована в брандмауэре.

Защита информации в системах связи

Две основные решаемые задачи здесь заключаются в предотвращении утечки информации при передаче ее по каналам связи и обеспечении взаимной аутентификации участников телекоммуникационного общения.

Первая задача решается использованием шифрования передаваемой информации. Построение и анализ систем шифрования информации является предметом *криптографии*. Как наука, а иногда и как искусство шифрования сообщений, криптография имеет многовековую историю. Развитие компью-

[165] Часто используется понятие «брандмауэр». Брандмауэр – программа, анализирующая весь поток данных, проходящий через сетевой адаптер. Руководствуясь установленными правилами, брандмауэр разрешает или отвергает прохождение пакетов данных.

терных систем телекоммуникаций, необходимость решения задач аутентификации и ряда других задач, связанных с обеспечением юридической значимости электронных документов и защитой от отказов привели в последнее время к развитию новых направлений в криптографии, связанных с решением такого рода задач.

Методы классической криптографии

Под шифрованием информации понимают такое ее преобразование, при котором противник или злоумышленник, получив доступ к такой преобразованной информации, не сможет ничего понять.

Никакой способ преобразования информации, или алгоритм, его реализующий, не может долго оставаться секретным. Поэтому современная концепция шифрования заключается в том, что шифр, или система шифрования, строятся на основе некоторого семейства преобразований *открытых текстов* в *закрытые* (шифрованные). Выбор конкретного преобразования каждый раз определяется некоторым параметром, который называется *ключом*. Ключ всегда секретен и известен только участникам шифрованного обмена информацией. Сами же преобразования открытых текстов в шифрованные тексты могут быть несекретными.

Таким образом, система шифрованного обмена информацией выглядит следующим образом. Отправитель сообщения шифрует открытый текст на некотором ключе, получает закрытый текст, или криптограмму, и посылает ее по каналу связи. Получатель тем же ключом расшифровывает закрытый текст и получает открытый. Третья заинтересованная сторона – противник, или злоумышленник, перехватив криптограмму, пытается дешифровать ее, то есть тем или иным способом определить открытый текст сообщения или ключ.

Основные требования, предъявляемые к шифрам, заключаются в следующем:

- ключей должно быть достаточно много, чтобы противник не смог при дешифровании сообщения перебрать все ключи в приемлемое время;
- алгоритм шифрования должен быть достаточно сложным, чтобы противостоять возможному его анализу и построению алгоритмов дешифрования.

Последнее требование характеризует центральный вопрос криптографии, которым является оценка стойкости применяемых алгоритмов шифрования, определяющая уверенность в том, что предполагаемый оппонент, не

имеющий доступа к используемому криптографическому ключу, не сможет дешифровать и понять смысл перехваченной шифрованной информации. Проведение исследований, позволяющих получить такую оценку, являются весьма трудоемким и дорогостоящим делом, посильным только профессиональному криптографу. Поэтому на практике рекомендуется использовать сертифицированные криптографические средства, прошедшие всесторонние исследования и аттестацию ФАПСИ[166].

Использование симметричных криптографических систем, то есть систем с одинаковым секретным ключом у отправителя и получателя сообщения, позволяют решать проблемы аутентификации и обеспечения целостности сообщения. Аутентификация отправителя достигается самим фактом получения сообщения, зашифрованного на ключе, известном только отправителю (и получателю). Проверка целостности сообщения обеспечивается добавлением в текст криптограммы некоторой дополнительной информации (*имитовставки*), играющей роль контрольной суммы. Контрольная сумма является функцией всего сообщения и секретного ключа. Целостность сообщения подтверждается совпадением значений контрольной суммы, вычисленной на передающем и приемном концах.

Системы с открытым распределением ключей

Одной из наиболее сложных задач защиты сетей является генерация и распространение криптографических ключей. В настоящее время наиболее перспективными представляются решения, связанные с гибридными криптосхемами, использующими традиционные методы шифрования с секретным ключом для защиты секретности и целостности, при одновременном использовании методов шифрования с открытым ключом для реализации функций распределения ключей (асимметричная криптография).

Способы открытого распределения ключей основаны на использовании так называемых односторонних функций. Односторонней функцией называется функция φ, значение $y = \varphi(N)$ которой сравнительно легко вычисляется при известном значении аргумента N, а вычисление аргумента N при извест-

[166] ФАПСИ – Федеральное агентство правительственной связи и информации. Создано в 1991 г. для обеспечения государственных организаций специальными видами связи и информации, а также криптографической и инженерно-технической безопасностью шифрованной связи в Российской Федерации и ее учреждениях за рубежом. Кроме того, ФАПСИ осуществляет государственный контроль за этой деятельностью.

ном значении функции y представляет собой сложную математическую или алгоритмическую задачу.

Алгоритм выработки общего секретного ключа для абонентов A и B может быть реализован с помощью следующих шагов:

- Для генерации пары ключей выполняются следующие действия:
  - выбираются два больших простых числа p и q, при этом $|p| \approx |q|$;
  - вычисляется их произведение $n = pq$;
  - вычисляется функция Эйлера $\varphi(N) = (p - 1)(q - 1)$
  - выбирается случайное целое число $1 < e < \varphi(N)$, взаимно простое с $\varphi(N)$;
  - с помощью расширенного алгоритма Эвклида находится число d такое, что $ed \equiv 1$.

Число n называется модулем, а числа e и d – открытой и секретной экспонентами. Пара чисел (N,e) является открытой частью ключа, а d – секретной. Числа p и q после генерации пары ключей могут быть уничтожены, но ни в коем случае не должны быть раскрыты.

- Чтобы зашифровать сообщение с длиной $m < N$, вычисляется

$$c = m^e \bmod N$$

Число c используется в качестве зашифрованного текста.

- Для расшифровки нужно вычислить следующее:

$$m = c^d \bmod N$$

Нетрудно убедиться, что при расшифровке будет восстановлено исходное сообщение:

$$c^d \equiv (m^e)^d \equiv m^{ed} \pmod N.$$

Из условия

$$ed \equiv 1 \bmod \varphi(N)$$

следует, что

$$ed = k\varphi(N) + 1$$

для некоторого целого числа k, следовательно,

$$m^{ed} \equiv m^{k\varphi(N) + 1} \bmod N.$$

Согласно теореме Эйлера:

$$m^{\varphi(N)} \equiv 1 \bmod N,$$

поэтому

$$m^{k\varphi(N)+1} \equiv m \bmod N$$

$$c^d \equiv m \bmod N$$

Стеганография

Стеганография – в дословном переводе с греческого означает «тайнопись». Это наука о скрытой передаче информации путем сохранения в тайне самого факта передачи. В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование.

Методы стеганографии использовались русскими революционерами в письмах из тюрем. Это были строки, написанные молоком между строк внешне безобидного обычного письма. Секретный текст проявлялся при проглаживании бумаги горячим утюгом. Использовались также различные химические препараты. Однако царская охранка знала об этой переписке и успешно прочитывала секретную переписку. Во время второй мировой войны активно использовались микроточки – микроскопические фотоснимки, вклеиваемые в текст писем, телеграмм.

В настоящее время под стеганографией чаще всего понимают скрытие информации в графических, аудио- либо текстовых файлах путем использования специального программного обеспечения.

Различают несколько направлений стеганографии, выделившиеся в конце 90-х годов:

- классическая стеганография;
- компьютерная стеганография – направление классической стеганографии, основанное на особенностях компьютерной платформы. Примеры – стеганографическая файловая система StegFS для Linux, скрытие данных в неиспользуемых областях форматов файлов, подмена символов в названиях файлов, текстовая стеганография и т. д.;
- цифровая стеганография – направление компьютерной стеганографии, основанное на скрытии информации в цифровых объектах, изначально имеющих аналоговую природу, то есть в изображениях, видео- и аудиофайлах.

Из рамок цифровой стеганографии вышло наиболее востребованное легальное направление – встраивание в мультимедиа-объекты цифровых водя-

ных знаков (watermarking), являющееся основой для систем защиты авторских прав и DRM-систем[167]. Методы этого направления настроены на встраивание скрытых маркеров, устойчивых к различным преобразованиям контейнера.

Аутентификация информации

Аутентификация информации является очень важным вопросом для всех абонентов государственных и коммерческих систем связи. Приобретающие все более важную роль новые виды электронного сервиса: электронная почта, электронная оплата счетов и т.д. делают проблему аутентификации информации на основе цифровой подписи все более значимой. Ведь никакие устройства, типа факса, не способны обеспечить подлинное авторство электронного документа в условиях жесткой модели аутентификации с несколькими возможными типами злоумышленников. Подпись эффективна только тогда, когда ее очень трудно подделать.

Стержень любой системы защиты – криптографические средства. Но часто компании терпят крах не из-за утечки информации, а из-за преднамеренной порчи их данных, навязывания им ложной информации.

В обычной почте письмо подписывается отправителем и заключается в конверт, что обеспечивает конфиденциальность, целостность содержания письма и подлинность авторства.

ISO использует термин «цифровая подпись» для методов, позволяющих устанавливать подлинность автора сообщения (документа) при возникновении спора относительно авторства этого сообщения. Любая схема цифровой подписи включает две процедуры:

- процедура формирования подписи (с помощью личного секретного ключа);
- процедура проверки (с помощью общеизвестной проверочной комбинации, называемой открытым ключом).

Только в случае успешного прохождения обеих процедур арбитр может разрешить возникший спор относительно авторства документа.

По сложившейся в связи традицию информацию, требующую опреде-

[167] DRM – Digital rights management, управление цифровыми правами. Программные или программно-аппаратные средства защиты авторских прав, затрудняющие создание копий защищаемых произведений (распространяемых в электронной форме), либо позволяющие отследить создание таких копий.

ления подлинности, будем называть сообщением. В самой общей модели аутентификации сообщения представлено пять участников: *отправитель* А, *получатель* В, *злоумышленник* С, *доверенная сторона* Д и *арбитр* Е. Поставлены задачи:

- отправителю – формирование и отправка сообщения Т;
- получателю – получение сообщения Е и установление его подлинности;
- доверенной стороне – документированная рассылка необходимой служебной информации абонентам вычислительной сети, чтобы в случае возникновения спора между А и В относительно авторства и подлинности сообщения представить необходимые документы в арбитражный суд;
- независимому арбитру Е – разрешение спора между абонентами А и В относительно подлинности сообщения Т.

Возможные способы обмана (нарушителем подлинности сообщения) при условии, что между участниками модели А, В, С отсутствует кооперация:

- А1 – отправитель А заявляет, что он не посылал сообщение Т получателю В, хотя в действительности его посылал;
- А2 – отправитель А заявляет, что он передал сообщение Т, хотя в действительности передал Т (подмена отправленного сообщения);
- В1 – получатель В изменяет полученное от А сообщение Т на Т’ и заявляет, что данное измененное сообщение он получил от отправителя А (подмена принятого сообщения);
- В2 – получатель В формирует свое сообщение Т и заявляет, что получил его от отправителя А (имитация принятого сообщения);
- С1 – злоумышленник С искажает сообщение, которое отправитель А передает получателю В (подмена передаваемого сообщения);
- С2 – злоумышленник С формирует свое сообщение Т и посылает получателю В от имени отправителя А (имитация передаваемого сообщения);
- С3 – злоумышленник С повторяет ранее переданное сообщение, которое отправитель А посылал получателю В (повтор ранее переданного сообщения).

Аутентификация при наличии взаимного доверия между участниками информационного обмена обеспечивается *имитозащитой* информации с помощью криптостойких преобразований. Имитозащита информации давно применяется в вычислительных сетях военного назначения. Так, например, в Министерстве финансов США имитозащита реализуется использованием

процедуры на основе криптографического алгоритма DES в режиме со сцеплением блоков и использованием кода MAC[168] для выработки контрольной комбинации – имитовставки).

В зарубежной литературе методы имитозащиты информации подразделяются на два типа.

1) *Методы типа MAC*, основанные на использовании кодов аутентификации сообщений. Эти коды могут быть использованы для контроля целостности как сообщений в каналах связи, так и файлов, хранящихся в памяти в *области недоверия*. При этом контрольная комбинация, полученная с помощью секретного ключа, передается (хранится) вместе с документом. Любое лицо, имеющее соответствующий секретный ключ, может проверить целостность документа. Злоумышленник, не имеющий секретного ключа, бессилен в попытке выдать ложный модифицированный документ за подлинный. Точнее, его успех будет определяться длиной контрольной комбинации, при соответствующем выборе которой вероятность успеха практически равна нулю. Контрольная сумма вычисляется как криптографическая функция от сообщения x и секретного ключа k, известного только определенным взаимодействующим пользователям (в нашем случае A и B). Пользователь A, для надежной передачи открытого сообщения x пользователю B, вычисляет проверочную комбинацию $y = F(k,x)$ и отправляет пользователю B в виде (x,y). В состав сообщения x входят данные, подлежащие передаче, и служебная информация (адрес отправителя, адрес получателя, дата, время отправки, номер сообщения). Пользователь B получает сообщение (x,y), вычисляет $F(k,x)$ и сравнивает результат вычисления с полученным значением y. По результатам сравнения делается вывод о подлинности полученного сообщения.

2) *Методы типа MDC*[169] основаны на использовании кодов, обнаруживающих обман. Они подразумевают вычисление контрольной комбинации от документа на основе использования односторонней хэш-функции. Понятие *односторонней хэш-функции* занимает центральное место в современной криптографии. В данный момент для реализации методов MDC используются два основных типа односторонних функций сжатия. Первый тип основан на нетрадиционном использовании криптографических алгоритмов типа DES, предполагающем подстановку вместо ключа блоков текста документа.

[168] MAC – Message authentication code, код аутентификации сообщения.
[169] MDC – Manipulation detection codes.

Второй тип предполагает использование алгоритмов, использующих следующий подход. Для осуществления контроля целостности сообщения пользователь заранее вычисляет значение хэш-функции и хранит его вместе с сообщением в зоне доверия. При необходимости проверки подлинности сообщения он заново вычисляет значение хэш-функции и сравнивает его с хранимым. При совпадении делается вывод о целостности. С точки зрения обычного пользователя метод очень удобен для контроля целостности файлов, хранящихся в области недоверия на жестком диске и дискетах, т.к. при его реализации нет необходимости заботиться о ключах. Использование MDC для защиты передаваемого сообщения было предложено национальным Бюро стандартов США. Для защиты передаваемого сообщения X пользователь A заранее вычисляет эталон – контрольную комбинацию $y = \varphi(x)$, а затем шифртекст $Z=E(k,k)$, где под $E(k,k)$ понимается шифрование на ключе k в режиме *гаммирования*[170]. Пользователь B, получив шифртекст Z, расшифровывает его, вычисляет $\varphi(x)$, сверяет результат этого вычисления с полученной проверочной комбинацией y, и по результатам этого сравнения делает вывод о целостности полученного сообщения.

Для аутентификации информации при отсутствии взаимного доверия между участниками информационного обмена в 1976 году была предложена концепция «цифровой подписи». Она заключается в том, что каждый абонент имеет свой секретный ключ и соответствующую ему проверочную комбинацию, которая по своему характеру является общедоступной. Цифровая подпись вычисляется на основе текста подписываемого сообщения и секретного личного ключа. Всякий желающий убедиться в подлинности сообщения использует для этого проверочную комбинацию. При этом знание проверочной комбинации не дает возможности подделать подпись. Такие схемы получили название *асимметричных криптографических систем аутентификации*.

Составными частями, обеспечивающими реализацию цифровой подписи являются:

- генерация секретного ключа с помощью датчика случайных ключей;
- выработка и опубликование открытого ключа;

[170] Гаммирование – преобразование исходного текста, при котором символы исходного текста складываются (по модулю, равному мощности алфавита) с символами псевдослучайной последовательности, вырабатываемой по определенному правилу. Шифр гаммирования – потоковый шифр, в котором для зашифровывания данных используется гаммирование.

- формирование подписи;
- проверка подписи.

Параметры цифровой подписи:

- стойкость схемы – определяется длиной подписи, длиной ключа и открытого ключа;
- количество и размер сообщений, подлежащих подписи. Этот параметр определяет лимит на число подписываемых на одном ключе сообщений.

Считается, что злоумышленник раскрыл схему подписи, если он вычислил секретный ключ и имитировал подпись хотя бы одного сообщения.

Сопоставление обычной и цифровой подписей:

1) обычная:

- каждая личность использует индивидуальные характеристики;
- попытка подделки определяется с помощью графологического анализа;
- подпись и подписываемый документ передаются только вместе на одном листе бумаги;
- копии подписанного документа не действительны, если они не имеют своей подлинной подписи;

2) цифровая подпись:

- каждая личность использует свой секретный ключ;
- сложность подделки подписи определяется сложностью вычисления ключа в используемом криптографическом алгоритме;
- цифровая подпись может передаваться отдельно от документа, т.к. она зависит от содержания документа и секретного ключа;
- не нужно подписывать каждую копию документа (по той же причине).

Защита юридической значимости электронных документов

Защита юридической значимости электронных документов необходима при использовании вычислительных сетей и сетей для обработки, хранения и передачи информационных объектов (сообщений, файлов, баз данных), содержащих в себе юридические документы: приказы, платежные поручения, контракты и другие распорядительные, договорные, финансовые документы. Их общая особенность заключается в том, что в случае возникновения споров (в том числе и судебных), должна быть обеспечена возможность доказательства истинности факта того, что автор действительно фиксировал акт своего воле-

изъявления в отчуждаемом электронном документе. Для решения данной проблемы могут использоваться современные криптографические методы проверки подлинности информационных объектов, связанные с применением цифровых подписей. На практике вопросы защиты юридической значимости электронных документов решаются совместно с вопросами защиты систем связи.

Защита информации от утечки по техническим каналам

Защита информации от утечки по техническим каналам является важным аспектом защиты конфиденциальной и секретной информации от НСД со стороны посторонних лиц, направленным на возможность утечки информативных электромагнитных сигналов за пределы охраняемой территории. При этом предполагается, что внутри охраняемой территории применяются эффективные режимные меры, исключающие возможность бесконтрольного использования специальной аппаратуры перехвата, регистрации и отображения электромагнитных сигналов. Для защиты широко используется экранирование помещений, а также технические меры, позволяющие снизить интенсивность информативных излучений самого оборудования ЭВМ и связи. В последнее время определенное распространение получил метод электромагнитной маскировки информативных сигналов.

В некоторых случаях необходима дополнительная проверка вычислительного оборудования на предмет возможного выявления специальных закладных устройств промышленного шпионажа, которые могут быть внедрены недобросовестным конкурентом с целью ретрансляции или записи информативных излучений компьютера, а также речевых и других несущих уязвимую информацию сигналов.

Защита информации от компьютерных вирусов

Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ актуальна ввиду больших масштабов «вирусных эпидемий», при которых заражаются сотни тысяч компьютеров. Особенно опасны вирусы для компьютеров, входящих в состав однородных вычислительных сетей. Как правило рассматриваются два направления в методах защиты от вирусов:

- применение «иммуностойких» программных средств, защищенных от возможности несанкционированной модификации (разграничение досту-

па, методы самоконтроля и самовосстановления);

- применение специальных программ-анализаторов, осуществляющих постоянный контроль возникновения «аномалий» в деятельности прикладных программ, периодическую проверку наличия других возможных следов вирусной активности (например обнаружение нарушений целостности программного обеспечения), а также «входной» контроль новых программ перед их использованием (по характерным признакам наличия в их теле вирусных образований).

Первое направление трудно реализуемо, второе наиболее часто употребляемо.

Защита от несанкционированного копирования

Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации ориентирована на проблему охраны интеллектуальной собственности, воплощенной в виде программ, ценных баз данных и других объектов авторского права и интеллектуальной собственности. Такая защита обычно осуществляется с помощью специальных программных средств, подвергающих защищаемые программы предварительной обработке (вставка парольной защиты, проверок по обращению к устройствам хранения ключа и ключевым дискетам, блокировка отладочных прерываний, проверка рабочей ЭВМ по ее уникальным характеристикам[171] и т.п.), которая приводит исполняемый код защищаемой программы в состояние, препятствующее его выполнению на «чужих» машинах. В некоторых случаях для повышения защищенности применяются дополнительные аппаратные блоки (ключи), подключаемые к разъемам компьютера, а также производится шифрование файлов, содержащих исполняемый код программы.

Общим свойством средств защиты информации от несанкционированного копирования является ограниченная стойкость такой защиты, так как в конечном случае исполнимый код программ поступает на выполнение в центральный процессор в открытом виде и может быть прослежен с помощью аппаратных отладчиков. Однако это не снижает потребительские свойства

[171] Примерно такая схема защиты от нелегального копирования реализована в операционной системе Windows Vista. Замена любого из основных компонентов компьютера (центральный процессор, материнская плата, сетевой адаптер и т.д.) может привести к необходимости заново регистрировать и активировать операционную систему.

средств защиты до нуля, так как основной целью их применения является если и не исключить, то хотя бы в максимальной степени затруднить возможность массового тиражирования новых программных средств до появления последующих изданий.

Авторское право

К признанию за человеком права на результаты своего творческого труда современная цивилизация шла не одно столетие. Высшим актом признания этого права стала Всеобщая декларация прав человека, принятая Генеральной Ассамблеей ООН 10 декабря 1948 года. В статье 27 Декларации говорится, что «каждый человек имеет право на защиту его моральных и материальных интересов, являющихся результатом научных, литературных или художественных трудов, автором которых он является»[172]. Более подробно содержание прав на результаты творческого труда было определено в специальном международном законодательстве, в частности, в Бернской конвенции 1886 года об охране литературных и художественных произведений, Международной Римской конвенции об охране прав производителей фонограмм и вещательных организаций[173], в Соглашении о торговых аспектах прав на интеллектуальную собственность.

В российском законодательстве понятие «интеллектуальная собственность» появилось в 1993 году с принятием закона РФ «Об авторском праве и смежных правах», который существенно пересмотрел существовавшее прежде представление об авторском праве. Но, хотя Закон об авторском праве и смежных правах действует уже более десяти лет, уровень правовой культуры в стране пока довольно низок. Кроме того, в силу ряда объективных и субъективных причин в России отношения, связанные с авторским правом, не развиты еще настолько, чтобы соответствовать общепринятой мировой практике.

В январе 2007 в России вступила в силу 4 часть Гражданского Кодекса, называющаяся «Права на результаты интеллектуальной деятельности и средства индивидуализации», который регулирует не только вопросы собственно интеллектуальной собственности, но и все действия и последствия, связанные с ней. Охраняемыми результатами интеллектуальной деятельности являются:

[172] http://www.un.org/russian/documen/declarat/declhr.htm.
[173] http://www.fips.ru/avp/law/inter/rome.htm.

- произведения науки, литературы и искусства;
- программы для ЭВМ;
- базы данных;
- исполнения;
- фонограммы;
- сообщения в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания);
- изобретения;
- полезные модели;
- промышленные образцы;
- селекционные достижения;
- топологии интегральных микросхем;
- секреты производства (ноу-хау);
- фирменные наименования;
- товарные знаки и знаки обслуживания;
- наименования мест происхождения товаров;
- коммерческие обозначения.

Согласно Гражданскому кодексу РФ, интеллектуальная собственность – это «исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполняемых работ или услуг (фирменное наименование, товарный знак, знак обслуживания и т.п.)».

Таким образом, интеллектуальная собственность распространяется на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации. Обладателями интеллектуальной собственности могут выступать гражданин или юридическое лицо. Основной характеристикой интеллектуальной собственности является то, что только обладатель интеллектуальной собственности, и в первую очередь автор, располагает исключительными правами на ее использование, а также то, что никакое иное лицо не может каким-либо способом использовать интеллектуальную собственность без его разрешения.

Авторское право, т.е. право автора на выраженное в материальном носителе произведение творческого труда, включает неимущественные права и имущественные права.

Неимущественными правами являются:

- право на авторство (право признаваться автором);
- право разрешать или запрещать использовать произведение под своим именем или псевдонимом;
- право разрешать или запрещать обнародование произведения;
- право защищать произведение от искажений или других посягательств.

Неимущественные права вечно остаются за автором. Ни по договору, ни по наследству эти права переходить к другим лицам не могут. Они не продаются и не покупаются.

Имущественные права – это право на воспроизведение, распространение, публичное исполнение, перевод, переделку произведения и т.д. Они по договору могут передаваться: на определенный срок; на весь срок охраны авторских прав; за вознаграждение или бесплатно; на исключительной или на неисключительной основах. Если права переданы на исключительной основе, то это означает, что только тот, кому переданы права на воспроизведение и распространение произведения, может ими пользоваться.

Личные неимущественные права автора не отнесены законодательством к интеллектуальной собственности. Имущественные права могут защищаться с помощью гражданских (возмещение убытков, взыскание штрафа, неустойки, принуждение к устранению допущенных нарушений) или специальных мер защиты, предусмотренных законом об авторском праве (конфискация контрафактных материалов, выплата компенсации от 10 до 50000 минимальных размеров оплаты труда; взыскание дохода вследствие нарушения авторских прав и другое).

Авторское право распространяется на произведения науки, литературы и искусства, как обнародованные, так и не обнародованные, выраженные в любой объективной форме, независимо от назначения и достоинства произведения. Произведение должно обладать следующими признаками:

- признак творческого характера произведения, то есть произведение является результатом творческого труда его автора;
- признак объективной формы произведения, то есть произведение существует в объективной форме (книги, видеозаписи, аудиозаписи, картины, рукописи и другое);
- признак содержания произведения, подразумевает ограничения, на-

лагаемые законодательством (например, недопустима пропаганда войны, бандитизма, геноцида, терроризма; разжигание расовой или национальной розни; порнография, призывы к свержению конституционного строя);

- признак обнародования произведения, то есть не важно, обеспечен к произведению свободный доступ других лиц или нет.

Закон об авторском праве не предусматривает совершения каких-либо специальных действий для возникновения авторского права на произведение. Авторское право на произведение возникает с момента его создания, дальнейшее осуществление и защита авторских прав могут производиться без каких-либо формальностей.

Однако в международном законодательстве предусмотрен ряд мер, которые автор может использовать для подтверждения принадлежности авторских прав на произведение: депонирование экземпляров, регистрация, оговорка о сохранении авторского права, нотариальные удостоверения, уплата сборов, изготовление или выпуск в свет экземпляров произведения на территории данного государства.

Для оповещения об исключительных имущественных правах их обладатель вправе использовать знак охраны авторских прав, который помещается на каждом экземпляре произведения и обязательно состоит из трех элементов:

- латинской буквы «с» в окружности – ©;
- имени (наименования) обладателя исключительных имущественных прав;
- года первого опубликования произведения.

Характерно, что данный знак не имеет никакого принципиального юридического значения, поскольку российское законодательство исходит из принципа презумпции авторского права, т. е. автором произведения считается то лицо, чье имя указано на произведении в качестве его автора, пока не доказано иное. Как правило, эти значки помогают другим заинтересованным лицам, желающим использовать это произведение, сориентироваться относительно настоящего (в данный момент времени) владельца исключительных авторских прав.

Лицом, обладающим неимущественными авторскими правами, может быть только автор. Обладателями исключительных имущественных авторских прав могут быть как физические, так и юридические лица. Приобрете-

ние таких прав может происходить либо в силу закона, либо по договору.

Владельцами исключительных имущественных авторских прав по закону являются:

- автор произведения;
- наследники умершего автора;
- наниматель (работодатель) автора служебного произведения;
- производитель аудиовизуального произведения;
- лицо, выпускающее в свет энциклопедии, энциклопедические словари и периодические издания (газеты, журналы и другое).

Кроме того, по договору владельцами исключительных имущественных авторских прав могут становиться любые лица, которым были переданы такие права другим лицами, которым эти права действительно принадлежали.

Срок действия авторского права установлен только для исключительных имущественных прав автора. Срок охраны распространяется на произведение в течение всей жизни автора и 50 лет после его смерти, за исключением случаев анонимных произведений и совместных произведений. Для анонимных произведений срок охраны авторских прав составляет 50 лет с момента опубликования. Но если автор произведения раскроет свое имя, то в отношении этого произведения начинает действовать обычный порядок исчисления сроков.

Личные неимущественные права автора охраняются бессрочно.

Закон об авторском праве устанавливает достаточно широкий перечень случаев, когда авторские имущественные права ограничиваются, при этом допускается использование произведений без согласия автора и без выплаты ему вознаграждения.

1. Воспроизведение произведения в личных целях без согласия автора и без выплаты авторского вознаграждения.

2. К использованию произведения без согласия автора и без выплаты авторского вознаграждения относятся также случаи частичного использования произведения:

- цитирование в оригинале и в переводе в научных, исследовательских, полемических, критических и информационных целях;
- использование произведений и отрывков из них в качестве иллюстраций в учебных целях;

- воспроизведение опубликованных в газетах или журналах статей по текущим экономическим, политическим, социальным и религиозным вопросам;
- воспроизведение публично произнесенных политических речей обращений, докладов и других аналогичных произведений в объеме, оправданном информационной целью;
- воспроизведение в обзорах текущих событий произведений, которые становятся увиденными или услышанными в ходе таких событий, в объеме, оправданном информационной целью.

3. Воспроизведение произведений без извлечения прибыли рельефно-точечным шрифтом или другими специальными способами для слепых, кроме произведений, специально созданных для таких способов воспроизведения.

4. Использование произведений путем репродуцирования (изготовления копий) библиотеками и архивами для замены испорченных экземпляров, для учебных или исследовательских целей.

5. Свободное использование произведений, постоянно расположенных в местах, открытых для свободного посещения.

6. Свободное публичное исполнение произведений на свадьбах, похоронах и так далее в объеме, оправданном характером мероприятия.

7. Свободное воспроизведение для судебных целей.

8. Свободная запись краткосрочного пользования, производимая организациями эфирного вещания.

9. Лицо, правомерно владеющее экземпляром программы для ЭВМ или базы данных, вправе без получения разрешения автора и без выплаты дополнительного вознаграждения осуществлять свободное воспроизведение программ для ЭВМ и баз данных для личных целей, а также осуществлять их декомпилирование.

Контрафактными являются экземпляры произведения, изготовление или распространение которых влечет за собой нарушение авторских прав. Слово «контрафактный» происходит от французского слова «contrefacon» – нарушение прав интеллектуальной собственности. Таким образом, «контрафактный» означает «нарушающий авторские или смежные права».

В настоящее время вместо слова «контрафактный» часто говорят «пи-

ратский», от английского неологизма «piracy»[174] – нарушение прав интеллектуальной собственности.

В области авторских прав на территории России действуют несколько организаций:

- Российское Авторское Общество (РАО), старейшая и самая крупная организация;
- Российское Общество Правообладателей в Аудиовизуальной Сфере (РОПАС). Его цель – собирать авторское вознаграждение для авторов в кинематографической сфере. РОПАС отслеживает использование их произведений не только на телевидении и в кинопрокате, но и при тиражировании видеокассет, других аудио-видео носителей, в сети Интернет;
- РОСП – Российское общество по смежным правам. Его задача – собирать вознаграждение за использование этих прав (то есть прав исполнителей, производителей фонограмм, организаций эфирного и кабельного вещания);
- РОМС – Российское общество по мультимедиа и цифровым сетям, его деятельность направлена на реализацию и защиту авторских прав в Интернет. РОМС выдает разрешения на несколько способов использования охраняемых объектов: радиовещание в Интернете, загрузка музыкальных файлов (с большими ограничениями), сообщения для всеобщего сведения путем размещения на WEB-страницах.

Существует также Российское Агентство по правовой охране программ для ЭВМ и баз данных. Его деятельность обоснована соответствующим законом Российской Федерации. Оно работает по несколько другим правилам. Так, например, в Законе о защите программ для ЭВМ и баз данных определяется обязательная регистрация программных продуктов в этом агентстве.

Авторское право в Интернете

Последние достижения в области цифровой технологии, наряду с быстрым развитием электронно-компьютерных сетей и других средств связи, являются серьезной проблемой для эффективной защиты авторских прав.

[174] Под компьютерным пиратством понимается несанкционированное копирование и распространение материала, защищённого авторским правом. Термин «пиратство» может быть применён к таким продуктам интеллектуального труда, как программное обеспечение, музыкальные композиции, фильмы, книги, компьютерные игры, топологии интегральных микросхем, товарные марки и марки обслуживания (trademark), доменные имена. Пиратство в большинстве стран рассматривается как противозаконная деятельность.

Любая работа, выполненная в двух измерениях, может быть преобразована в цифровую форму, а затем храниться и использоваться в цифровом формате. Это резко увеличивает легкость и скорость ее копирования, качество копий, возможности манипуляций и изменения работы, а также скорость, с которой ее копии могут использоваться любым желающим.

На использование авторских произведений в Интернете распространяются общие положения законодательства об авторском праве. Использование произведения в Интернет осуществляется в рамках тех имущественных прав автора, которые уже закреплены в законе об авторском праве.

3.4. Стандартизация методов обеспечения безопасности

С созданием современных коммуникационных технологий резко возросла роль унификации и стандартизации элементов и алгоритмов сетей. Особую роль стандартизация играет при обеспечении безопасности связи в каналах телекоммуникаций.

Работы по стандартизации безопасности связи в основном были начаты после 1980 года. За сравнительно короткий срок были получены достаточно важные результаты в области стандартизации, чему способствовала активная деятельность международных организаций по стандартизации архитектуры сетей ЭВМ, принципов взаимодействия открытых систем и протоколов передачи данных. В первую очередь это относится к таким организациям, как:

- Международное телекоммуникационное сообщество, ITU (International Telecommunication), – специальное агентство при ООН, объединяющее 164 страны;
- Международный консультационный комитет по телеграфным и телефонным коммуникациям, МККТТ, являющийся одним из отделений ITU;
- Международная организация стандартизации.

Эти организации являются головными по разработке стандартов и рекомендаций по передаче информации в целом и по обеспечению безопасности связи в частности.

Вопросами стандартизации занимается также и ряд других международных организаций:

- Международный электротехнический комитет[175];

[175] IEC – The International electrotechnical commission, Швейцария, Женева.

- Европейская ассоциация производителей ЭВМ[176];
- Европейская ассоциация почтовых и телекоммуникационных управлений[177];
- Координационный совет по исследованию сетей[178].

Определенное влияние на процессы стандартизации оказывают национальные организации по стандартизации ряда развитых стран.

Очень важна координирующая роль международных организаций, поскольку одни и те же стандарты одновременно разрабатываются различными организациями в разных странах. Так, например, стандарты для локальных вычислительных сетей разрабатывают Институт инженеров по электротехнике и радиоэлектронике, Европейская ассоциация производителей ЭВМ и множество национальных комитетов по стандартизации. Некоторые из этих стандартов становятся международными через ISO.

Стандарты IEEE рассматриваются как стандарты США и могут быть представлены МОС через Американский национальный институт стандартов ANSI.

Стандарты для локальных вычислительных сетей реального времени разрабатываются Приборостроительным обществом Америки (ISA).

Стандарты на локальные вычислительные сети для автоматизации учреждений разрабатывает Комитет 802 IEEE. Им разработан также вариант объединенного стандарта ANSI и IEEE. Кроме того, ISO присвоила этому документу статус проекта международного стандарта.

Разработка и утверждение стандартов на международном и национальном уровнях являются достаточно длительным процессом. Поэтому крупные фирмы, не дожидаясь появления международных стандартов, объединяются для выработки собственных промышленных стандартов на коммуникационные протоколы.

В США вопросы стандартизации сосредоточены в трех известных организациях: Министерстве обороны (военные стандарты), Министерстве торговли (финансовые стандарты) и Администрации (федеральные стандарты). Одним из головных разработчиков военных стандартов является Центр национальной безопасности, многие разработки которого признаны стандартами. Можно от-

[176] ECMA – The European computer manufactures association.
[177] CEPT – Conference europeene des administration de postes et des telecomunication.
[178] CCRN – The Coordinating council on research networks.

метить, в частности, стандарты по таким известным программам, как «закрытая сеть связи передачи данных» и «Правительственный вариант взаимодействия открытых систем». Решая главную задачу по разработке единого критерия безопасности (защиты) ЭВМ, Центр разработал систему стандартов в области компьютерной безопасности, включающую следующие части:

- «Критерий оценки безопасности компьютерных систем», – так называемая «Оранжевая книга»;
- «Программа оценки безопасности продуктов»;
- «Руководство по применению критерия оценки безопасности компьютерных систем в специфических средах», – так называемая «Желтая книга»;
- комплект документов под общим названием «Радужная серия», включающий разъяснение критериев оценки безопасности компьютерных систем для безопасных сетей, для безопасных СУБД и для отдельных подсистем безопасности.

Особый интерес по сохранению коммерческой тайны представляют финансовые стандарты. Необходимо отметить, что финансовая область является самой большой из тех, где огромные средства тратятся на засекречивание информации. Это относится прежде всего к системе секретной электронной передачи денег. Финансовые ведомства ведут большую работу в этом направлении и разрабатывают множество стандартов засекречивания. Для финансовой службы наибольший интерес представляют следующие направления обеспечения безопасности:

- целостность сообщений. Для этой цели финансовые стандарты используют зашифрованные способы подтверждения или специальный код подтверждения целостности сообщения;
- конфиденциальность;
- скрытность ввода;
- организация шифра. Является существенным элементом любой системы, использующей шифрование.

3.5. Информационная безопасность в распределенных системах

Модель безопасности

В соответствии со стандартами ECMA ключевая концепция модели безопасности для открытых распределенных систем заключается в использо-

вании информации о полномочиях. Она генерируется определенными службами безопасности в ответ на аутентификационные запросы и затем используется другими службами для разрешения или запрещения определенной деятельности.

При построении модели сделано предположение об отсутствии защищенных объектов. Защищенными предполагаются только службы и инфраструктура безопасности. *Инфраструктура безопасности* – часть инфраструктуры распределенной системы, управляющая безопасностью. Информация о полномочиях, передаваемая в распределенной системе, упакована и защищена от нежелательного использования. После получения она проверяется получателем (обычно одной из служб безопасности) и используется для определения прав доступа. В этом случае информация о полномочиях использована для распространения доверия и привилегий в распределенной системе.

Система защиты в распределенной системе включает в себя три *кольца защиты*[179]. Первое кольцо отделяет пользователей от распределенной системы. Сама распределенная система находится внутри первого кольца защиты и состоит из объектов, которые являются субъектами управления безопасностью.

Второе кольцо безопасности окружает каждый из объектов, входящих в состав распределенной системы. Все взаимодействия объектов контролируются, а взаимодействия, требующие услуг безопасности, осуществляются через инфраструктуру безопасности, к которой эти объекты находятся.

Третье кольцо безопасности окружает внутренние составляющие каждого объекта (данные и возможность вычислений). Модель позволяет объектам иметь свое внутреннее управление доступом, обеспечивая объекты необходимой информацией и дополнительными услугами. В безопасность, обеспечиваемую объектом самим по себе, инфраструктура не вмешивается, за исключением требований создателя объектов. Классификация служб безопасности может быть представлена следующим образом.

Службы безопасности:

- информация о полномочиях:
  - служба аутентификации;
  - служба атрибутов;
  - служба обмена между областями безопасности;

[179] Кольцо защиты – абстрактное понятие, подразумевающее аппаратные или программные методы разграничения доступа к определенным ресурсам.

- управление безопасностью:
  - служба безопасного взаимодействия;
  - служба авторизации;
- слежение за безопасностью:
- служба сбора информации о безопасности.

Основное назначение службы аутентификации – получение от пользователя некоторых опознавательных знаков, их проверка и выдача мандата. Служба атрибутов предназначена для чтения мандата или установки проверяемых привилегий. Служба обмена обеспечивает взаимодействие между разными доменами (с различными политиками безопасности и различными администраторами). Служба безопасного взаимодействия обеспечивает безопасную связь между двумя любыми объектами системы, независимо от того, в какой области безопасности они находятся. Назначение службы авторизации – принимать решения по управлению доступом. Класс служб слежения за безопасностью обеспечивает внутреннее слежение и управление безопасностью в распределенной системе в целом.

Существенной особенностью модели является то, что она не зависит от любой политики безопасности или механизма управления доступом.

Защита информации в Windows

Разработчики Windows (версии NT, 2000, XP и далее) разместили в нулевом кольце защиты только самую важную часть кода ОС – исполняемый модуль. Остальные компоненты ОС обладают меньшими привилегиями. Это отличает Windows от, например, NetWare 3.x, в которой создаваемые загрузочные модули могут исполняться даже в нулевом кольце, нарушая при этом защиту данных.

Принципиально важным в Windows является то, что в основу взаимодействия прикладной программы и ОС заложена модель «клиент–сервер». Все обращения пользовательской программы (клиента) к ОС переадресуются ядром для обработки специальной программе (серверу), называемой защищенной подсистемой. При этом используется механизм, аналогичный вызову удаленной процедуры[180], что позволяет легко перейти от взаимодействия между процессами в пределах одной машины к распределенной системе.

[180] RPC – remote procedure call, один из основных механизмов взаимодействия в распределенных системах.

Разрабатывая свою защищенную подсистему, программист имеет все преимущества пользовательского режима – стандартные компиляторы и мощные отладчики. Полностью отлаженная программа запускается в защищенном режиме.

Важным компонентом Windows являются защищенные подсистемы, выполняемые в непривилегированном пользовательском режиме. При этом категорически запрещен доступ пользовательских программ к аппаратуре – регистрам внешних устройств[181].

Встроенный в ядро Windows монитор защиты обеспечивает единый механизм проверки прав доступа к любым ресурсам системы. Тем самым исключается возможность несанкционированного доступа к информации и обеспечивается высокая степень ее защиты. В этом проявляется отличие данной ОС от некоторых других, где такая проверка осуществляется программным модулем, работающим на менее защищенном уровне аппаратных привилегий микропроцессора. При этом Windows не только контролирует доступ к любым ресурсам, но и протоколирует все действия администратора и пользователей, направленные на нарушение защиты.

Как и в большинстве многопользовательских систем, в Windows имеется учетная база, содержащая имена пользователей и рабочих групп (к которым принадлежит тот или иной пользователь), а также пароли. Перед началом работы необходимо для авторизации сообщить свое имя и пароль, в противном случае доступ в систему не предоставляется.

Очень важна для Windows концепция домена. Домен – это объединение нескольких компьютеров, с общей учетной базой пользователей и единой стратегией обеспечения безопасности. Пользователь может зарегистрироваться на любом из компьютеров домена. Каждый домен имеет по крайней мере один сервер имен, на котором администратор централизованно ведет учетную базу пользователей. Возможно объединение доменов друг с другом на основе «взаимного доверия», при этом они администрируются отдельно, но учетные данные пользователей одного из соединенных доменов действительны во всех остальных.

[181] В отличие от операционных систем DOS и Windows 95/98/Me, в которых такой доступ разрешался, более того, иногда был единственным способом взаимодействия со специфической аппаратурой.

В отличие от DOS, где любой пользователь «сам себе администратор», в Windows права и возможности пользователя и администратора четко распределены. Все пользователи разбиты на группы, различающиеся привилегиями доступа к системе. Наиболее широкими полномочиями обладают члены группы администраторов[182]. В то же время, принадлежность к этой группе не дает права доступа к любой информации на диске. Если пользователь снял право доступа администратора к своим файлам, то последний не сможет их использовать. Правда, администратор может получить доступ к файлу, воспользовавшись своим правом поменять его владельца, но система запротоколирует это действие и не позволит восстановить прежние атрибуты файла, а значит, владелец будет оперативно извещен о попытке несанкционированного доступа.

Защита информации в ОС UNIX

Идентификаторы пользователя и группы. Пользователи, которым разрешено входить в систему, перечислены в учетном файле пользователей **`/etc/passwd`**. Пользователи объединяются в группы, перечисленные в учетном файле **`/etc/group`**. Каждому пользователю и группе назначается идентификатор. Пользователь или группа пользователей могут быть снабжены паролем.

Учетный файл пользователей **`/etc/passwd`** играет большую роль в многопользовательской защите. Это текстовый файл, каждая строка которого соответствует одному пользователю и может содержать информацию следующего характера: имя пользователя, зашифрованный пароль, идентификатор пользователя, идентификатор группы, первоначальный текущий каталог, имя выполняемого файла, используемого в качестве интерпретатора команд.

Когда пользователь входит в систему, отыскивается строка в учетном файле пользователей. Если поле пароля пусто, пароль не запрашивается. Поскольку пароль хранится в зашифрованном виде, чтение файла разрешается всем, что делает возможным использование этого файла, например, для преобразования идентификатора пользователя в его имя.

[182] Максимальные привилегии в Windows имеет учетная запись LOCALSYSTEM, с правами которой запускаются некоторые системные процессы. Они имеют доступ к любым файлам и ресурсам, даже закрытым пользовательским (за исключением зашифрованных, поскольку в этом случае требуется пароль для расшифровки). Однако пользователю или администратору не предоставляется возможность доступа в систему с правами этой записи.

Наличие последнего поля позволяет пользователю выбрать программу, которая будет заменять стандартный интерпретатор команд shell. Если это поле пусто, используется shell.

С каждым процессом связаны два идентификатора: идентификатор пользователя и идентификатор группы пользователей. Процесс, созданный для интерпретации команд, вводимых с конкретного терминала, получит эти идентификаторы от пользователя после его подключения к системе на терминале. Порожденный процесс наследует идентификаторы от породившего процесса.

С каждым файлом также связаны идентификаторы пользователя и группы, унаследованные от процесса, создавшего файл. Пользователь и группа, идентификаторы которых связаны с файлом, считаются его владельцами. В дальнейшем при определенных условиях их можно менять.

Идентификаторы пользователя и группы, связанные с процессом, определяют его права при доступе к файлам. По отношению к конкретному файлу все процессы делятся на три категории:

- владелец файла – ему соответствуют процессы, имеющие идентификатор пользователя, совпадающий с идентификатором владельца файла;
- члены группы файла – им соответствуют процессы, имеющие идентификатор группы, совпадающий с идентификатором группы, которой файл принадлежит;
- прочие – им соответствуют процессы, не попавшие в первые две категории.

Процессы могут иметь три способа доступа к файлу: чтение, запись, выполнение. При исполнении этих запросов ядро системы проверяет, разрешен ли требуемый доступ к указанному файлу.

Код защиты файла. При создании файлу присваивается код защиты – слово, биты которого характеризуют тип файла и права доступа процессов к нему.

Если процесс требует доступа к файлу, определяется категория, в которую он попадает по отношению к этому файлу. Затем из кода защиты выбираются биты, соответствующие данной категории, и проверяется, разрешен ли требуемый доступ. Если доступ не разрешен, системный вызов отвергается ядром.

Привилегированный пользователь. Привилегированный пользователь имеет идентификатор, равный нулю. Процесс, с которым связан нулевой иден-

тификатор, считается привилегированным. Независимо от кода защиты файла привилегированный процесс имеет право доступа к любому файлу для чтения и записи. Если в коде защиты хотя бы одной категории пользователей (процессов) разрешено выполнять файл, привилегированный процесс тоже имеет право выполнять этот файл. Как правило, в учетном файле пользователей имеется привилегированный пользователь с именем *root*. Привилегированный пользователь должен быть защищен паролем в учетном файле пользователей.

Эффективные и реальные идентификаторы. Обычно при вызове выполняемого файла сохраняются связанные с ним идентификаторы пользователя и группы. Однако возможно временно заменить ранее связанные с процессом идентификаторы на идентификаторы владельцев этого файла. Управляют такой заменой биты кода защиты файла:

Первоначальные идентификаторы, связанные с процессом, называются реальными; идентификаторы, полученные им после выполнения системного вызова, – эффективными. Таким образом, сначала эффективные идентификаторы совпадают с реальными. После выполнения системного вызова эффективный идентификатор пользователя (или группы), если смена идентификатора выполняемого файла разрешена, полагается равным идентификатору владельца (или группы) выполняемого файла.

Права доступа процесса проверяются по его эффективным идентификаторам. Процесс может узнать связанные с ним реальные и эффективные идентификаторы и динамически их изменить. Поскольку это означает изменение прав процесса, изменение идентификаторов разрешено только привилегированному процессу и такому процессу, реальный идентификатор которого совпадает с устанавливаемым.

Контрольные вопросы к разделу

1. Что понимают под защитой информации? Рассмотрите различные категории защиты информации с точки зрения основных направлений ее обеспечения.
2. В чем достоинства и недостатки технических средств получения, хранения, преобразования, отображения и передачи информации с точки зрения ее безопасности? Предложите способы снижения влияния таких недостатков и повышения роли этих достоинств при организации вычислительных сетей.
3. Объясните смысл понятий «идентификация», «аутентификация» и «авторизация». Проанализируйте роль этих понятий в обеспечении безопасно-

сти вычислительных систем и информационных ресурсов.

4. Дайте определение методам криптографии. Какие подходы можно применять для сокрытия информации, и чем определяется применимость этих подходов и методов?
5. Что представляет собой асимметричная криптография? Покажите использование простейшего из алгоритмов на конкретном примере шифрования и дешифрования фрагмента текста. Какие применения находят системы с открытым распределением ключей?
6. Перечислите правовые аспекты использования информации в вычислительных сетях. С каким сложностями юридического плана сталкивается пользователь глобальной сети?
7. Что такое авторское право? Каковы предпосылки его возникновения и как обстоит ситуация с ним на сегодняшний день? Как, по-вашему, будет развиваться обстановка с авторским правом в ближайшие годы и в более отдаленном будущем?
8. Каким образом решаются вопросы обеспечения безопасности информации в распределенных системах? Как вы думаете, возможно ли кардинальное изменение обстановки в этой области в течение ближайших лет?

ПРИЛОЖЕНИЯ

1. Список национально-политических доменов первого уровня

Страна или территория	Домен
А	
Австралия	au
Австрия	at
Азербайджан	az
Албания	al
Алжир	dz
Американское Самоа	as
Ангилья	ai
Ангола	ao
Андорра	ad
Антарктика	aq
Антигуа и Барбуда	ag
Аомынь (Макао)	mo
Аргентина	ar
Армения	am
Аруба	aw
Афганистан	af
Б	
Багамские острова	bs
Бангладеш	bd
Барбадос	bb
Бахрейн	bh
Белиз	bz
Белоруссия	by
Бельгия	be
Бенин	bj
Бермудские острова	bm
Болгария	bg
Боливия	bo
Босния и Герцеговина	ba
Ботсвана	bw
Бразилия	br
Британская территория в Индийском океане	io
Бруней	bn
Буркина Фасо	bf
Бурунди	bi
Бутан	bt
В	
Вануату	vu
Ватикан (город-государство)	va
Венгрия	hu
Венесуэла	ve
Виргинские острова (Великобритания)	vg
Виргинские острова (США)	vi
Восточный Тимор	tp
Вьетнам	vn
Г	
Габон	ga
Гаити	ht
Гайана	gy
Гамбия	gm
Гана	gh
Гваделупа	gp
Гватемала	gt
Германия	de
Гибралтар	gi
Гондурас	hn
Гренада	gd
Гренландия	gl
Греция	gr
Грузия	ge
Гуам	gu
Д	
Дания	dk
Джибути	dj
Доминика	dm
Доминиканская республика	do
Е	
Египет	eg
З	
Заир, теперь Демократическая республика Конго[183]	zr
Замбия	zm
Западная Сахара	eh
Зимбабве	zw
И	
Израиль	il
Индия	in
Индонезия	id
Иордания	jo
Ирак	iq
Иран	ir
Ирландия	ie
Исландия	is
Испания	es
Италия	it
Й	
Йемен	ye
К	
Кабо-Верде	cv
Казахстан	kz
Камбоджа	kh
Камерун	cm

[183] Так как Заир переименован в Демократическую республику Конго, домен .zr упразднен.

Страна или территория	Домен
Канада	ca
Катар	qa
Кения	ke
Кипр	cy
Киргизстан	kg
Кирибати	ki
Китай	cn
Кокосовые (Килинг) острова	cc
Колумбия	co
Коморские острова	km
Конго	cg
Конго, Демократическая республика	cd
Корейская Народно-Демократическая Республика	kp
Коста Рика	cr
Кот д'Ивуар	ci
Куба	cu
Кувейт	kw
Л	
Лаос	la
Латвия	lv
Лесото	ls
Либерия	lr
Ливан	lb
Ливия	ly
Литва	lt
Лихтенштейн	li
Люксембург	lu
М	
Маврикий	mu
Мавритания	mr
Мадагаскар	mg
Майотта	yt
Македония	mk
Малави	mw
Малайзия	my
Мали	ml
Мальдивские острова	mv
Мальта	mt
Марокко	ma
Мартиника	mq
Маршалловы острова	mh
Мексика	mx
Микронезия	fm
Мозамбик	mz
Молдавия	md
Монако	mc
Монголия	mn
Монтсеррат	ms
Мьянма	mm
Н	
Намибия	na
Науру	nr
Непал	np
Нигер	ne
Нигерия	ng

Страна или территория	Домен
Нидерландские Антилы	an
Нидерланды	nl
Никарагуа	ni
Ниуэ	nu
Новая Зеландия	nz
Новая Каледония	nc
Норвегия	no
Нормандские острова, Гернси	gg
Нормандские острова, Джерси	je
О	
Объединеные Арабские Эмираты	ae
Оман	om
Остров Буве	bv
Остров Вознесения	ac
Остров Мэн	im
Остров Норфолок	nf
Остров Рождества	cx
Остров Святой Елены	sh
Острова Кайман	ky
Острова Кука	ck
Острова Малые Отдаленные (США)	um
Острова Теркс и Кайкос	tc
Острова Уоллис и Футуна	wf
Острова Херд и Макдональд	hm
Острова Шпицберген (Свальбард) и Ян-Майен	sj
П	
Пакистан	pk
Палау	pw
Палестина	ps
Панама	pa
Папуа - Новая Гвинея	pg
Парагвай	py
Перу	pe
Питкэрн	pn
Польша	pl
Португалия	pt
Пуэрто-Рико	pr
Р	
Реюньон	re
Российская Федерация - Россия	ru
Руанда	rw
Румыния	ro
С	
Сальвадор	sv
Самоа	ws
Сан-Марино	sm
Сан-Томе и Принсипи	st
Саудовская Аравия	sa
Свазиленд	sz
Северные Марианские острова	mp
Сейшельские острова	sc
Сенегал	sn
Сен-Пьер и Микелон	pm
Сент-Винсент и Гренадины	vs
Сент-Китс и Невис	kn

Страна или территория	Домен
Сент-Люсия	lc
Сингапур	sg
Сирия	sy
Словакия	sk
Словения	si
Соединенное Королевство Великобритании	uk
Соединенные Штаты Америки	us
Соломоновы острова	sb
Сомали	so
Союз Советских Социалистических Республик[184]	su
Судан	sd
Суринам	sr
Сьерра-Леоне	sl
Сянган (Гонконг)	hk
Т	
Таджикистан	tj
Тайвань, провинция Китая	tw
Тайланд	th
Танзания	tz
Того	tg
Токелау (Юнион)	tk
Тонга	to
Тринидад и Тобаго	tt
Тувалу	tv
Тунис	tn
Туркменистан	tm
Турция	tr
У	
Уганда	ug
Узбекистан	uz
Украина	ua
Уругвай	uy
Ф	
Фарерские острова	fo
Фиджи	fj
Филиппины	ph
Финляндия	fi
Фолклендские (Мальвинские) острова	fk
Франция	fr
Французская Гвиана	gf
Французская Полинезия	pf
Французские южнополярные территории	tf
Х	
Хорватия	hr
Ц	
Центральноафриканская республика	cf
Ч	
Чад	td
Чехия	cz
Чили	cl
Ш	
Швейцария	ch
Швеция	se
Шри-Ланка	lk
Э	
Эквадор	ec
Экваториальная Гвинея	gq
Эритрея	er
Эстония	ee
Эфиопия	et
Ю	
Югославия, теперь Сербия и Черногория	yu
Южная Георгия и Южные Сандвичевы острова	gs
Южная Корея	kr
Южно-Африканская республика	za
Я	
Ямайка	jm
Япония	jp

[184] Союз Советских Социалистических Республик прекратил свое существование в декабре 1991 года, но в доменной зоне *su* к тому времени уже было зарегистрировано много доменных имен. Поэтому она поддерживалась в статическом состоянии больше десяти лет. В 2003 году зона *su* была расконсервирована и снова введена в коммерческую эксплуатацию. Таким образом, Российская Федерация – единственная страна в мире, являющаяся обладателем сразу двух доменных зон.

2. Смайлики и пояснения к ним

Одной из проблем при общении посредством электронной почты является необходимость по возможности более точно и в максимально краткой форме донести до собеседника эмоции, которые вкладываются в письмо. С этой целью на заре существования телекоммуникационных сетей были придуманы символы для обозначения эмоций и состояния человека, которые получили название *смайлики*. Автор этой идеи неизвестен, но популяризация смайликов произошла во многом благодаря сети Fidonet, а в последнее время – коротким текстовым сообщениям[185], повсеместно используемым при переписке по мобильной связи. Смайлики читаются при мысленном повороте текста на 90 градусов по часовой стрелке.

Существует несколько сотен смайликов, порой весьма затейливых. Ниже приведен более или менее полный перечень основных смайликов, встречающихся в текстах. Характерно, что в последнее время наиболее популярные смайлики уже попадаются не только в периодической литературе и средствах массовой информации, но и в книжных изданиях.

---

[185] SMS – Short message service, служба коротких сообщений. Система, позволяющая посылать и принимать текстовые сообщения при помощи сотового телефона. Технология SMS поддерживается основными сотовыми сетями (GSM, NMT, DAMPS, CDMA). Также SMS-сообщения на телефоны можно отправлять из интернета и других сетей (пейджинговых, X.25 и др.), используя специальные протоколы. Текст может состоять из алфавитно-цифровых символов, максимальный размер сообщения в стандарте GSM — 140 байт. При использовании 7-битной кодировки (только латинский алфавит и цифры) максимальная длина сообщения – 160 символов. При использовании 8-битной кодировки (включая немецкий, французский алфавит) максимальная длина – 140 символов. Для поддержки других национальных алфавитов (китайского, арабского, русского и др.) используется 2-байтная кодировка UTF-16, при этом максимальная длина сообщения – 70 символов. Стандартом предусмотрена возможность отправления сегментированных сообщений, таким образом максимальная длина сообщения значительно увеличивается. Однако каждый сегмент обычно тарифицируется как отдельное сообщение.

В России многие абоненты сотовых сетей предпочитают писать SMS-сообщения на родном языке, используя латинские буквы, что первоначально было обусловлено отсутствием поддержки кириллицы телефонными аппаратами, а позже – привычкой, возможностью написать более длинные сообщения, а также использовать устоявшиеся аббревиатуры (см. приложение 3).

Смайлик	Описание
:-)	обычная улыбка
;-)	улыбка с подмигиванием
:-(	рассерженная, хмурая, печальная физиономия
:-I	индифферентное выражение
:-/	скептическое выражение
:-P	высовывающий язык
:-()	выражение удивления
%-(I)	смеюсь
%-)	веселое недоумение
%-\	полное недоумение
%-{	усатая вариация недоумения
&:-)	затейливая прическа
'-)	одноглазый
':-)	челка набок
(-:	австралиец
(-::-)	сиамские близнецы
(-_-)	инопланетянин
(8-)	в шлеме
(:-)	лысый

Смайлик	Описание
(:-*	поцелуй
(:=)	двухносый
)	чеширский кот
!#!^*&:-)	шизофреник
o-)	циклоп
*-(	циклоп с проткнутым глазом
*<|:-)	дед мороз
+-(:-)	священник
+<||-)	рыцарь
+O:-)	поп
,-)	подмигивающий одноглазый
- -:-)	панк
0:-)	ангел
3:-o	корова
8)	лягушка
8-O	паника
8-]	скепсис
8:-)	маленькая девочка
:-) 8	большая девочка

3. Основные сокращения, принятые при общении в сети

Наподобие смайликам, призванным передать собеседнику некоторую эмоциональную нагрузку сообщения, в сетях и сообщениях SMS часто используются аббревиатуры, образовавшиеся при сокращении характерных английских фраз, зачастую выражающих отношение собеседника к той или иной сентенции, высказанной кем-либо. Ниже приведен список наиболее часто употребимых аббревиатур с их раскрытой формой и переводом. Отметим при этом, что написание интернет-аббревиатур с прописных букв не принципиально, часто пишут только строчными, либо вообще вразнобой – кому как нравится.

Сокращение	Раскрытая форма	Перевод
10X	Thanks	Спасибо
2	To	К
4	For	Для
4GET	Forget	Забудь
AAMOF	As a matter of fact	Как факт
ADDY	Address	Адрес
ADN	Any day now	Теперь в любой день.

Сокращение	Раскрытая форма	Перевод
AFAIK	As far as i know	Насколько я знаю
AFK, AFTK	Away from the keyboard	Вдали от клавиатуры, т.е. меня нет за клавиатурой
AISE	As I see it	Как мне кажется
AKA	Also known as	Еще известен как
ANY1	Any one	Каждый
AOP	Authorized operator	Авторизированный оператор
AS	On another subject	По другому вопросу (беседы)
ASAP	As soon as possible	Быстро, как только возможно
ASL	Age/sex/location	Возраст, пол, место жительства
ATM	At the moment	В данную минуту, сейчас
ATSL	Along the same line	В той же строке
BB	Bye bye	До встречи
BBIAF	Be back in a few minutes	Вернусь через несколько минут
BBIAH	Be back in an hour	Вернусь через час
BBIAM	Be back in a minute	Вернусь через минуту
BBIAS	Be back in a second	Вернусь через секунду
BBL	be back later	буду позже
BBS	Be back soon	Скоро вернусь
BCNU	Be see in' you	Еще увидимся
BE4	Before	Перед
BF	Boyfriend	Любимый парень
BION	Believe it or not	Хотите верьте, хотите нет
BNF	Big name fan	Большой фанат
BOC	But of course	Но конечно
BRB	Be right back	Сейчас вернусь..
BTW	By the way	Между прочим, кстати
C	See	Вижу (видишь)
CMIIW	Correct me if I am wrong	Поправьте меня, если я ошибаюсь
CU	See you	Увидимся
CUL	See you later	Увидимся позже
DIIK	Damned if i know	Будь я проклят, если знаю
EM	Them	Им
EMFBI	Excuse me for butting in	Простите, что вмешиваюсь
F2F	Face to face	С глазу на глаз, тет а тет
FAQ	Frequently asked questions	Часто задаваемые вопросы
FITB	Fill in the blank	Заполни пробелы
FUBAR	Fouled up beyond all repair	Полностью испорчено
FUD	Fear, uncertainty and doubt	Страх, неуверенность, сомнение
FW	Freeware	Бесплатно
FWIW	For what it's worth	А зачем это нужно ?
FYI	For your information	Информация для вас
GF	Girlfriend	Любимая девушка
GIWIST	God, i wish i'd said that	Боже, это должен был сказать я!
GN	Good night	Доброй ночи
GR8	Great	Восхитительно
GTG	I got to go	Я должен идти

Сокращение	Раскрытая форма	Перевод
H8	Hate	Ненавидеть
HHOS	Ha-ha only serious	Ха-ха, только я серьезно
HSIK	How should i know	Откуда мне знать?
HTH	Hope this helps!	Надеюсь, это поможет
IAAL	I am a lawyer	Я юрист
IANAL	I am not a lawyer	Я не юрист
IC	I see	Понятно, понял(а), понимаю
IIRC	If i recall correctly	(если я правильно помню)
IMCO	In my considered opinion	По моему продуманному мнению
IMHO	In my humble opinion	По моему скромному мнению
IMNSHO	In my not so humble opinion	По моему нескромному мнению
IMO	In my opinion	По моему мнению
IOW	In other words	Другими словами
IRL	In real life	В настоящей жизни
ITSFWI	If the shoe fits, wear it	Куй железо, пока горячо
JK	Just kidding	Просто шутка
K	OK	Хорошо
KNYF	Know how you feel	Понимаю твои чувства
L8R	Later	Позже
LOL	Laughing out loud	Громко смеюсь
LTNS	Long time no see	Давно не виделись
LTNT	Long time no type	Долго не писал
LTR	Long term relationship	Длительные отношения
M8	Mate	Товарищ
ME2	Me too	Я тоже
MF	Male or female	Мужчина или женщина
MYOB	Mind your own business	Оставь меня (их, нас) в покое
NO1	No one	Ни один
NOYB	None of your business	Не вашего ума дело
NP	No problems	Нет проблем
NRN	No response necessary	Отвечать необязательно
NTYMI	Now that you mention it	Теперь к вашему вопросу
OIC	Oh, i see	О, я вижу!
ONNA	Oh no, not again	О нет, только не снова!
OOTQ	Out of the question	Нет вопросов, разумеется
OTOH	On the other hand	С другой стороны
OTTOMH	Off the top of my head	Мне это не по зубам
PLZ	Please	Пожалуйста
PMJI	Pardon my jumping in	Прошу прощения, что я вмешиваюсь
POV	Point of view	Точка зрения
PPL	People	Обращение ко всем, находящимся на канале
R	Are	Быть
RL	Real life	Настоящая жизнь
ROFL	Rolling on the floor laughing	Кататься по полу от смеха
RSN	Real soon now	Действительно скоро
RTFAQ	Read the FAQ!	Почитай FAQ
RTFM	Read the following manual	Почитай руководство

Сокращение	Раскрытая форма	Перевод
SF	Science fiction	Научная фантастика
SMT	Something	Что-то
SOOHF	Sence of humor failure	Подвело чувство юмора
SOW	Speaking of which	Говоря о котором
SUP	What's up	Как дела?
SW	Shareware	Условно бесплатно
SWAK	Sealed with a kiss	Скрепленный поцелуем
SY	Sincerely yours	Искренне ваш
SYS	See you soon	Скоро увидимся (до встречи)
TANJ	There ain't no justice	Нет здесь справедливости
TFHAOT	Thank for help ahead of time	Заранее благодарен
TGAL	Think globally, act locally	Думать широко, действовать в рамках
TIC	Tongue in cheek	Язык за зубами
TNX	Thanks	Спасибо
TOBG	This oughta be good	Это [должно быть] хорошо
TPTB	The powers that be	Силы, которые есть
TTBOMK	To the best of my knowledge	На пределе моих знаний
TTUL	Talk to you later	Поговорим позже
U	You	Ты
U2	You too	Ты тоже
UC	You see	Видишь ли
W8	Wait	Ждать
wb	Welcome back	С возвращением
WBR	With best regards	Сердечный привет
WBW	With best wishes	С наилучшими пожеланиями
WRT	With respect to	С уважением
WTF	What the fruit	Что за черт?
YGLT	You're gonna love this	Тебе понравится
YMMV	Your mileage may vary	В вашем случае может быть по-другому

Некоторые специфичные слова, применяемые при общении в чатах, сервисах мгновенных сообщений, на интернет-форумах и IRC-каналах, перечислены ниже.

Слово	Описание
away	Статус пользователя, означает, что он отошел, занят или по какой-то иной причине не уделяет внимание происходящему на канале.
ban	Удаление пользователя с канала на длительный срок (от нескольких часов до неопределенного времени), используется операторами для поддержания порядка.

bot	Сокращение от «robot» – специальная программа, выполняющая автоматически или по заданному расписанию какие-либо действия через те же интерфейсы, что и обычный пользователь. В сервисах общения бот – программа, запущенная на удаленном компьютере, способная автоматически реагировать на различные действия, фразы и т.п. на канале (например, на нецензурные выражения). В его функции входит идентификация пользователей, модерирование канала в отсутствие оператора и т.д
flame	Бурное обсуждение какой-либо темы, часто переходящее во взаимные оскорбления.
flood	Ситуация, когда во время обсуждения какой-либо темы разговор уходит в совершенно иное русло, не относящееся к обсуждаемому вопросу. Также под флудом иногда подразумевается бесполезный разговор, болтовня, треп.
kick	Временное удаление пользователя с канала, используется операторами для поддержания порядка.
lag	Задержка прохождения информации между клиентом и сервером, например, промежуток времени от отправления сообщения до момента, когда его увидят другие участники беседы.
moder, op	Сокращения от слов «moderator» и «operator». Модератор (оператор) – человек, в обязанности которого входит поддержание порядка на IRC-канале, форуме или в чате.
private	Частная беседа между двумя пользователями.
sysop	Сокращение от «system operator» – системный оператор. Под системой изначально имелась ввиду BBS, поэтому «сисопом» был оператор BBS, а пользователи BBS были «юзерами». Позже «сисопами» стали называть операторов узлов в сети Fidonet. В дальнейшем термин получил более широкое значение, когда под «системой» стала пониматься не BBS, а операционная система компьютера. Слово «сисоп» стало почти синонимом понятия «системный администратор» и даже «пользователь» в применении к домашним компьютерам.

4. Языки разметки

Документы, находящиеся в Интернете и возвращаемые по протоколам HTTP, GOPHER, Z39.50 и другим, могут быть различными по своему содержанию. Но, как правило, все они сводятся к двум основным категориям по принципу представления данных: бинарный документ и текстовый документ. Бинарные документы – это программы, видео, звуковая и графическая информация, а также файлы баз данных и бинарные файлы прикладных программ. Текстовый документ – это обычный текстовый файл, который может быть прочитан и отображен при помощи самых простых средств.

Можно условно принять, что отдельные фрагменты текста, отмеченные заранее условленными символами, отображаться не будут, а тем или иным образом повлияют на способ отображения текста. Так, для перевода

строки служит символ с кодовым номером 13, и он обычно не отображается как отдельный символ.

Развитие этой идеи приводит к созданию специализированных языков разметки текста. Для отображения таких размеченных текстов применяются специальные программы, получившие название «браузеры».

В начале 60-х годов XX в. был создан язык SGML[186], утвержденный как международный стандарт в 1986 году. Незначительная популярность SGML обусловлена тем, что этот язык достаточно сложен.

SGML – это обобщенный метаязык, позволяющий строить системы логической и структурной разметки любых разновидностей текстов. Управляющие элементы (или *теги*), вносимые в текст при такой разметке, не несут никакой информации о внешнем виде документа, а лишь указывают границы и соподчинение его составных частей, т.е. задают его логическую структуру.

Для интерпретации текста, размеченного SGML, необходим специальный DTD-файл[187], в котором описаны все элементы разметки языка. Существование DTD позволяет автору документа создавать свои уникальные теги. Браузеру необходимо только указать путь к DTD-файлу, и он становится способен адекватно отображать SGML-документ.

В 1991 году сотрудник CERN Тим Бернес-Ли разработал DTD, который был «вмонтирован» в браузер, содержал небольшое количество тегов и предназначался для разметки технической документации. Так появился на свет HTML. Таким образом, HTML, является одной из реализаций SGML.

С момента создания HTML постоянно развивался. Изначально он разделял все особенности идеологии SGML, и разметка была чисто логической. Но начиная с версии языка 3.0 возникло серьезное противоречие между изначальным стандартом и потребностями пользователей, заинтересованных в гибких и богатых возможностях визуального представления и не желающих разбираться в структуре и логике DTD. Поэтому было введено новое средство, названное *CSS*[188]. CSS формально независимы от HTML, имеют совершенно иной синтаксис, не наследуют никаких идеоло-

[186] Standardized generalized markup language – универсальный стандартизованный язык разметки.

[187] Document type definition – документ определения типа.

[188] Cascading style sheets – каскадные таблицы стилей.

гических ограничений и позволяют задавать параметры визуального представления для любого тега HTML.

Но несмотря на попытки привести спецификации HTML к изначальной идеологии SGML, последние версии HTML весьма далеки от начальной концепции языка, и он все больше превращается в язык оформления документа. К тому же, набор тегов HTML весьма ограничен и не дополняем.

Поэтому был разработан язык XML[189]. Он также, как и HTML, является SGML-приложением. Однако в отличие от HTML, позволяет создавать собственные DTD (то есть, фактически, собственные теги), не содержит средств для оформления документа, и в отличие от SGML достаточно прост и удобен. Хотя и не настолько прост, как HTML.

Использование XML в последнее время существенно расширилось в связи с тем, что он оказался весьма удобен как универсальное средство хранения параметров и настроек программных приложений, а также организации интерфейса. Например, в браузере Mozilla интерфейс, реализующий доступ к изменению параметров программы полностью сделан на основе XML.

[189] Extensible markup language – расширяемый язык разметки.

АЛФАВИТНЫЙ УКАЗАТЕЛЬ

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Мухутдинов, Э. А. Информационные системы: учебн. пособие. / Э. А. Мухутдинов, Р. Г. Тахавутдинов. – Казань: КГЭУ, 2005. – 80 с.
2. Ситников, С. Ю. Технологии и протоколы компьютерных сетей: учебн. пособие. / С. Ю. Ситников. – Казань: КГЭУ, 2002.
3. Ситников, С. Ю. Системы передачи данных и сети ЭВМ: учебн. пособие. / С. Ю. Ситников. – Казань: КГЭУ, 2002.
4. Ситников, С. Ю. Волоконно-оптические линии связи: учебн. пособие. / С. Ю. Ситников. – Казань: Казан. гос. энерг. ун-т, 2003.
5. Малюк, А. А. Введение в защиту информации в автоматизированных системах. / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. – М., 2004. – 147 с.
6. Галатенко, В. А. Основы информационной безопасности: курс лекций. / В. А. Галатенко. – М., 2003. – 280 с.
7. Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации: учебн. пособие. / В. Л. Бройдо. – СПб, 2003. – 688 с.
8. Запечников, С. В. Основы построения витруальных частных сетей: учебн. пособие. / С. В. Запечников, Н. Г. Милославская, А. И. Толстой. – М., 2003. – 249 с.
9. Олифер, В. Г. Сетевые операционные системы: учебн. пособие. / В. Г. Олифер, Н. А. Олифер. – М., 2003. – 539 с.
10. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. / В. Г. Олифер, Н. А. Олифер. – М., 2004. – 864 с.
11. Пескова, С. А. Сети и телекоммуникации: учебник. / С. А. Пескова, А. В. Кузин, А. Н. Волков. – М., 2005. – 448 с.
12. Таненбаум, Э. Компьютерные сети. / Э. Таненбаум. – СПб.: Питер, 2003. – 992 с.
13. Мухутдинов, Э. А. Изучение основ языка SQL: лабораторный практикум. / Э. А. Мухутдинов. – Казань: КГЭУ, 2005. – 56 с.
14. Прокофьев, И. В. Защита информации в компьютерных сетях. / И. В. Прокофьев. – Москва: МИЭМ, 2003.