Глава восьмая

Компьютерные сети, Интернет, компьютерная безопасность

8.1. Компьютерные сети

При физическом соединении двух и более компьютеров образуется *компьютерная сеть*. В общем случае, для создания компьютерной сети необходимо специальное аппаратное обеспечение (*сетевое оборудование*) и специальное программное обеспечение (*сетевые программные средства*). Для персональных моделей ПК сетевое оборудование обычно интегрировано в состав системной платы компьютера, а сетевые программные средства входят в состав операционной системы.

Назначение компьютерных сетей

Создание компьютерной сети имеет целью совместное использование ресурсов или совместный доступ к ним. В данном случае слово *ресурс* — очень емкое. В зависимости от назначения сети в него вкладывают различный смысл.

Сетевые ресурсы бывают трех типов: *аппаратные, программные* и *информационные*. Например, устройство печати (принтер) — это аппаратный ресурс. Когда все участники небольшой компьютерной сети пользуются общим принтером, они обобщают аппаратный ресурс. То же можно сказать и о сети, имеющей *файловый сервер*, на котором все участники сети хранят свои архивы и результаты работы.

Помимо аппаратных ресурсов, компьютерные сети позволяют совместно использовать *программные ресурсы*. Так, например, для выполнения очень сложных и продолжительных расчетов можно подключиться к удаленной большой ЭВМ и передать ей вычислительное задание, а по окончании расчетов получить их результат.

Данные, хранящиеся на удаленных компьютерах, образуют *информационный ресурс*. Роль этого ресурса сегодня видна наиболее ярко на примере Интернета, который многими воспринимается, прежде всего, как гигантская информационно-справочная система.

Наши примеры с делением ресурсов на аппаратные, программные и информационные достаточно условны. На самом деле, при работе в компьютерной сети любого типа одновременно происходит совместное использование всех типов ресурсов. Так, например, обращаясь в Интернет за справкой, мы безусловно используем чьи-то аппаратные средства, на которых работают чужие программы, обеспечивающие поставку затребованных нами данных.

Основные понятия компьютерных сетей

Основными задачами, решаемыми при создании компьютерных сетей, являются:

- обеспечение совместимости оборудования по электрическим и механическим характеристикам;

- обеспечение совместимости программного и информационного обеспечения по системе кодирования и формату данных.

Решение этих задач относится к области стандартизации и основано на модели взаимодействия открытых систем OSI (Open System Interconnections). Данная модель была разработана и утверждена Международным институтом стандартизации ISO (International Standards Organization) и называется моделью ISO/OSI.

Модель ISO/OSI

Согласно модели ISO/OSI, архитектуру компьютерных сетей рассматривают на нескольких уровнях. Обмен данными в такой модели происходит в три этапа: сначала в передающем устройстве данные перемещаются с верхнего уровня на нижний, затем они транспортируются к принимающему устройству и, наконец, в принимающем устройстве поднимаются с нижнего уровня на верхний (рис. 8.1).

Самый верхний уровень — прикладной. На этом уровне люди обмениваются информацией. Самый нижний уровень — физический, на нем устройства обмениваются друг с другом сигналами. Между верхним и нижним уровнями располагаются промежуточные уровни. На этих уровнях информация циркулирует в форме данных, причем на каждом уровне — свой формат данных.

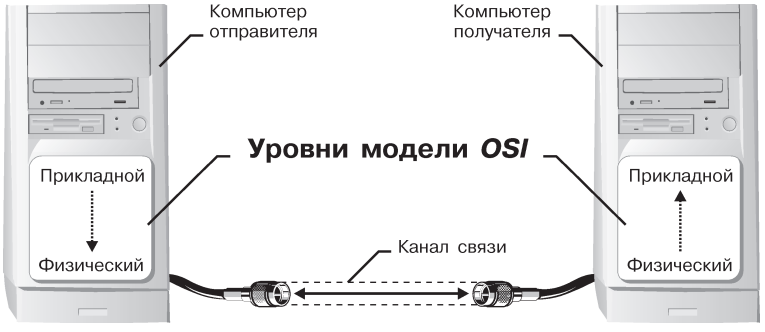

Рис. 8.1. Простейшая модель обмена данными в компьютерной сети

Протоколы связи

Для обеспечения необходимой совместимости на каждом из уровней компьютерной сети действуют свои стандарты, называемые протоколами. Аппаратные протоколы определяют характер взаимодействия устройств сети, а программные протоколы определяют условия взаимодействия программ и данных. Аппаратные устройства, обеспечивающие соблюдение протоколов, называют интерфейсами. А программные средства, играющие эту роль, называют программными протоколами или просто протоколами.

Так, например, если два компьютера соединены между собой, на физическом уровне протокол их взаимодействия определяют конкретные устройства физического порта и механические компоненты (разъемы, кабель и т. п.). На более высоких уровнях взаимодействие между компьютерами определяют программные средства, управляющие передачей данных через эти порты.

Локальные сети (LAN)

В соответствии с используемыми протоколами компьютерные сети принято разделять на локальные и глобальные. Характерная особенность локальной сети (LAN — Local Area Network) заключается в том, что все ее участники на нижних уровнях модели ISO/OSI используют единый комплект протоколов. Единство протоколов в элементах локальной сети обычно обеспечивается благодаря тому, что все они имеют общего собственника. Соответственно, сети этого вида имеют выраженную территориальную локализацию в пределах одного помещения, здания, группы компактно расположенных зданий.

Глобальные сети (WAN)

Глобальные сети (WAN — Wide Area Network), как правило, имеют неопределенные территориальные размеры, а их элементы могут принадлежать неопределенному кругу собственников. Глобальные сети связывают между собой как отдельные компьютеры, так и отдельные локальные сети, в том числе и использующие различные протоколы на нижних уровнях модели ISO/OSI.

Рабочая группа

Группы сотрудников, работающих над одним проектом в рамках локальной сети, называются рабочими группами. Одна локальная сеть может связывать несколько рабочих групп.

Политика сети

У участников рабочих групп могут быть разные права для доступа к общим ресурсам сети. Совокупность приемов разделения и ограничения прав участников компьютерной сети называется политикой сети.

Администрирование сети

Управление сетевыми политиками (их может быть несколько в одной сети) называется администрированием сети. Лицо, управляющее организацией работы участников локальной компьютерной сети, называется системным администратором.

Создание локальных сетей характерно для отдельных предприятий или их отдельных подразделений. Если же предприятие размещается на обширной территории, то его подразделения могут взаимодействовать через глобальные сети. В этом случае локальные сети подключаются к глобальной сети на основе договора присоединения, после чего присоединенные сети становятся частью глобальной сети.

Сетевой мост

Простейшее устройство для соединения между собой двух локальных сетей, использующих одинаковые протоколы, называется мостом. Мост может быть аппаратным (специализированный компьютер) или программным. Цель моста — не выпускать за пределы локальной сети данные, предназначенные для внутреннего потребления. Вне сети такие данные становятся «сетевым мусором», впустую занимающим каналы связи.

Сетевой шлюз

Для связи между собой нескольких локальных сетей, работающих по разным протоколам, служат специальные средства, называемые шлюзами. Шлюзы могут быть как аппаратными, так и программными. Например, это может быть специальный компьютер (шлюзовой сервер), а может быть и программа, установленная на обычный компьютер.

Сетевая безопасность

При подключении локальной сети предприятия к глобальной сети важную роль играет понятие сетевой безопасности. В частности, должен быть ограничен доступ в локальную сеть для посторонних лиц извне, а также ограничен выход за пределы локальной сети для сотрудников предприятия, не имеющих соответствующих прав.

Сетевой экран. Брандмауэр

Для обеспечения сетевой безопасности между локальной и глобальной сетью устанавливают так называемые сетевые экраны, или брандмауэры. Брандмауэром может быть устройство или программа, препятствующая несанкционированному перемещению данных между сетями.

8.2. Сетевые службы, основные понятия

Понятие виртуального соединения

Между участниками информационного обмена всегда существует физическая связь через материальные среды или средства. Однако в общественных отношениях рассматривать информационные связи через физические соединения не очень удобно. Например, корреспондентов из Москвы и Владивостока совершенно не интересуют технические детали сообщения между этими городами. Им совершенно все равно, будет ли почтовая бандероль доставлена самолетом или поездом: главное, чтобы она попала в руки адресата в заданный срок. Поэтому в общественных отношениях обычно вместо понятия физического соединения между участникам связи используют понятие виртуального соединения.

Рассмотрим простой пример взаимодействия двух корреспондентов с помощью обычной (не электронной) почты. Если они регулярно обмениваются письмами, то между ними действует виртуальное соединение. Оно было бы физическим, если бы каждый лично относил письмо партнеру и вручал в собственные руки, а не бросал его в почтовый ящик.

Сбором корреспонденции из общественных почтовых ящиков занимаются местные почтовые службы. Это следующий уровень модели связи. Далее, чтобы наше письмо достигло адресата в другом городе, должна существовать связь между нашей местной почтовой службой и его местной почтовой службой. Это еще один пример виртуальной связи, поскольку никакой физической связью эти службы не обладают — поступившую почтовую корреспонденцию они только сортируют и передают на уровень федеральной почтовой службы.

Федеральная почтовая служба в своей работе опирается на службы очередного уровня, например на почтово-багажную службу железнодорожного ведомства. И только рассмотрев работу этой службы, мы найдем, наконец, признаки физического соединения, например железнодорожный путь, связывающий два города.

Это очень простой пример, поскольку в реальности даже доставка обычного письма может затронуть гораздо большее количество служб. Но нам важно обратить внимание на то, что в нашем примере образовалось несколько виртуальных соединений между аналогичными службами, находящимися в пунктах отправки и приема. Не вступая в прямой контакт, эти службы взаимодействуют между собой. На каком-то уровне письма укладываются в мешки, мешки пломбируют, к ним прикладывают сопроводительные документы, которые где-то в другом городе изучаются и проверяются на аналогичном уровне.

Модель взаимодействия открытых систем ISO/OSI

Выше мы сказали, что согласно рекомендациям Международного института стандартизации системы компьютерной связи рекомендуется рассматривать на семи разных уровнях. Теперь мы рассмотрим, как именно в этой модели происходит обмен данными между удаленными пользователями.

1. **Прикладной уровень.** На этом уровне пользователь работает с конкретным приложением. С помощью текстового процессора, графического редактора или иной прикладной программы он создает некое сообщение, содержащее нужную информацию.
2. **Уровень представления.** Этот уровень относится уже не к отдельной прикладной программе, а ко всей операционной системе компьютера в целом. На этом уровне информация, составляющая сообщение, представляется данными заданного формата. Происходит это одним из двух возможных способов: либо сохранением сообщения (в виде файла данных), либо внесением сообщения в базу данных (в виде записи базы данных).
3. **Сеансовый уровень.** Протоколы этого уровня проверяют права пользователя на подключение к сети, и если с правами все в порядке, передают документ к протоколам транспортного уровня. Если по условиям информационного обмена требуется обеспечение безопасности, на этом уровне происходит дополнительная операция: шифрование сообщения и приложение к нему сертификата электронной цифровой подписи (ЭЦП).
4. **Транспортный уровень.** Программы, обеспечивающие функционирование данного уровня, преобразуют числовые данные сообщения так, как это принято для используемой сети. При этом сообщение нарезается на небольшие пакеты стандартного размера. Каждый пакет получает заголовок с номером, который позволит восстановить сообщение на принимающем компьютере.
5. Протоколы **сетевого уровня** отвечают за маршрут движения данных в сети. Если на транспортном уровне сообщение было нарезано на пакеты, то на сетевом уровне каждый пакет должен получить адрес, по которому произойдет его доставка.

6. **Уровень соединения.** На этом уровне происходит переход от данных, представляющих сообщение, к сигналам, представляющим данные. Сигналы модулируются в соответствии с данными, полученными с сетевого уровня. В компьютере эти функции модуляции выполняет сетевой адаптер или модем.
7. **Физический уровень.** Реальный информационный обмен происходит на физическом уровне. Здесь нет ни документов, ни пакетов, ни даже байтов — только сигналы. Однако из этих сигналов принимающий компьютер способен выделить информационные биты и далее восстановить байты данных и воспроизвести сообщение. Восстановление информации происходит постепенно, при переходе с нижнего на верхний уровень модели OSI на принимающем компьютере.

Особенности виртуальных соединений

Разные уровни протоколов сервера и клиента не взаимодействуют друг с другом напрямую: они взаимодействуют через физический уровень. Постепенно переходя с верхнего уровня на нижний, данные непрерывно преобразуются, «обрастают» дополнительными данными, которые анализируются протоколами соответствующих уровней на сопредельной стороне. Это и создает эффект виртуального взаимодействия уровней между собой. Однако, несмотря на виртуальность, это все-таки соединения, через которые тоже проходят данные.

Это очень важный момент с точки зрения компьютерной безопасности. Одновременно с теми запросами на поставку данных, которые клиент направляет серверу, передается масса служебной информации, которая может быть как желательной, так и нежелательной. Например, обязательно передаются данные о текущем адресе клиента, о дате и времени запроса, о версии его операционной системы, о его правах доступа к запрашиваемым данным и пр. Передается и немало косвенной информации, например о том, по какому адресу он посылал предыдущий запрос. Известны случаи, когда даже передавались идентификационные коды процессоров компьютеров.

На использовании виртуальных соединений основаны такие позитивные свойства электронных систем связи, как возможность работать по одному физическому каналу сразу с несколькими серверами. Но на них же основаны и такие негативные средства, как «троянские программы». Троянская программа — это вредоносная программа, создающая во время сеансов связи виртуальные соединения для передачи данных о компьютере, на котором установлена. Среди этих данных может быть парольная информация, информация о содержании жесткого диска и т. п. В отличие от обычных компьютерных вирусов, троянские программы не производят разрушительных действий на компьютере и потому они лучше маскируются.

Сетевые службы

На виртуальных соединениях основаны все службы современного Интернета. Так, например, пересылка сообщения от сервера к клиенту может проходить через десятки различных компьютеров. Это совсем не означает, что на каждом компьютере сообщение должно пройти через все уровни — ему достаточно «подняться» до

сетевого уровня (определяющего адресацию) при приеме и вновь «опуститься» до физического уровня при передаче. В данном случае служба передачи сообщений основывается на виртуальном соединении сетевого уровня и соответствующих ему протоколах (рис. 8.2).

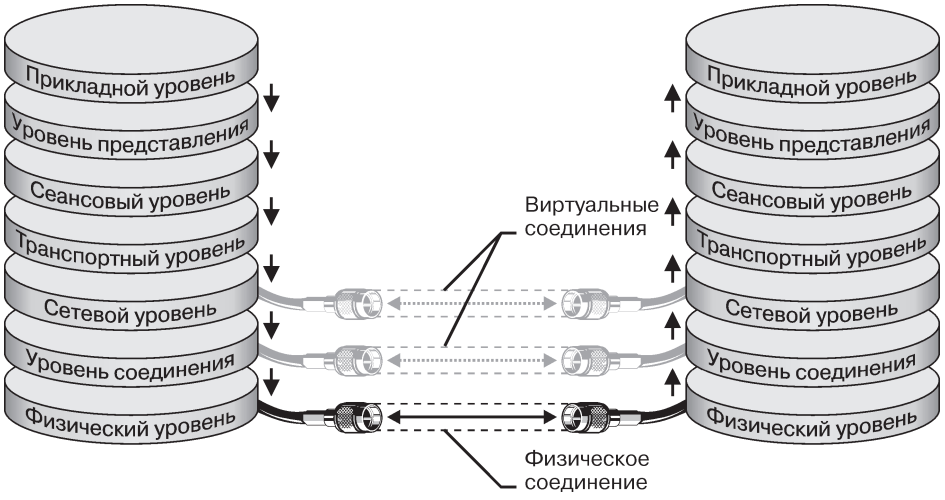

Рис. 8.2. Простейшая модель службы передачи сообщений

8.3. Интернет. Основные понятия

В дословном переводе на русский язык *интернет* — это *межсеть*, то есть в узком смысле слова интернет — это объединение сетей. Однако в 90-е годы XX века у этого слова появился и более широкий смысл: Всемирная компьютерная сеть. Интернет можно рассматривать в физическом смысле как сотни миллионов компьютеров, связанных друг с другом всевозможными линиями связи, однако такой «физический» взгляд на Интернет слишком узок. Лучше рассматривать Интернет как некое информационное пространство.

Интернет — это не совокупность прямых соединений между компьютерами. Так, например, если два компьютера, находящиеся на разных континентах, обмениваются данными в Интернете, это совсем не значит, что между ними действует одно прямое или виртуальное соединение. Данные, которые они посылают друг другу, разбиваются на пакеты, и даже в одном сеансе связи разные пакеты одного сообщения могут пройти разными маршрутами. Какими бы маршрутами ни двигались пакеты данных, они все равно достигнут пункта назначения и будут собраны вместе в цельный документ. При этом данные, отправленные позже, могут приходить раньше, но это не помешает правильно собрать документ, поскольку каждый пакет имеет свою маркировку.

Таким образом, Интернет представляет собой как бы «пространство», внутри которого осуществляется непрерывная циркуляция данных. В этом смысле его можно сравнить с теле- и радиоэфиром, хотя есть очевидная разница хотя бы

в том, что в эфире никакая информация храниться не может, а в Интернете она перемещается между компьютерами, составляющими *узлы сети*, и какое-то время хранится на их жестких дисках.

Ранняя история Интернета

Ранние эксперименты по передаче и приему информации с помощью компьютеров начались еще в 50-х годах и имели лабораторный характер. В США решение о создании первой глобальной сети национального масштаба было принято в 1958 году. Оно стало реакцией на запуск в СССР первого искусственного спутника Земли.

Поводом для создания глобальной компьютерной сети стала разработка Пентагоном глобальной системы раннего оповещения о пусках ракет (*NORAD* — North American Aerospace Defense Command). Станции системы NORAD протянулись через север Канады от Аляски до Гренландии, а подземный командный центр расположился вблизи города Колорадо-Спрингс в недрах горы Шайенн. Центр управления был введен в действие в 1964 году, и, собственно, с этого времени можно говорить о работе первой централизованной глобальной компьютерной сети.

Курированием работы сети NORAD занималось Управление перспективных разработок министерства обороны США DARPA (Defense Advanced Research Project Agency). Ему было поручено преодолеть основной недостаток централизованной сети: недостаточную устойчивость, связанную с тем, что при выходе из строя какого-либо из узлов полностью выходил из строя и весь сектор, находившийся за ним, а при выходе из строя центра управления выходила из строя вся сеть. Во времена ядерного противостояния сверхдержав этот недостаток был критичным.

Основными направлениями исследований DARPA стали поиск новых протоколов обслуживания сети и новых принципов сетевой архитектуры. Первая вневедомственная национальная компьютерная сеть получила название ARPANET. Ее внедрение состоялось в 1969 году.

В 70-е годы развитие сети ARPANET происходило за счет подключения региональных сетей, воссоздающих общую архитектуру ARPANET на более низком уровне (в региональном или локальном масштабе). В этот период основной задачей ARPANET стала координация групп коллективов, работающих над едиными научно-техническими проектами, а основной функцией стал обмен электронной почтой и файлами с научной и проектной документацией. Одновременно продолжалась разработка новых сетевых протоколов, способных обеспечить живучесть глобальной сети даже в ядерном конфликте.

Внедрение протоколов TCP/IP

Всякий раз, когда мы говорим о вычислительной технике, нам надо иметь в виду принцип единства аппаратного и программного обеспечения. Пока глобальное расширение ARPANET происходило за счет механического подключения все новых и новых аппаратных средств (узлов и сетей), до Интернета в современном понимании этого слова было еще очень далеко.

Рождение Интернета в современном понимании произошло в 1983 году, когда была решена проблема устойчивости глобальной сети. Это произошло благодаря внедрению протоколов TCP/IP, лежащих в основе Всемирной сети по нынешний день. Решив эту задачу, управление DARPA прекратило свое участие в проекте и передало управление сетью Национальному научному фонду (NSF), который в США играет роль Академии наук. Так в 1983 году образовалась глобальная сеть NSFNET. В середине 80-х к ней начали активно подключаться академические и научные сети других стран, например академическая сеть Великобритании JANET (Joint Academic Network).

Образование системы доменных имен

Годы, когда глобальной сетью руководил Национальный научный фонд США, вошли в историю как эпоха решительной борьбы с попытками коммерциализации сети. Сеть финансировалась на правительственные средства. Национальный научный фонд распределял их между узлами и материально наказывал тех, кто пытался иметь от сети побочные доходы. В то же время развитие сети после внедрения протокола TCP/IP значительно ускорилось, NSF уже не успевал отслеживать деятельность каждого узла, а с подключением иностранных секторов его роль стала чисто символической.

Во второй половине 80-х годов произошло деление Всемирной сети на домены по принципу финансирования. Узлы домена GOV финансировались на средства правительства, а узлы доменов SCI и EDU — на средства научных учебных организаций. При этом особую роль приобрел домен COM (коммерческий). Он не финансировался никем, то есть его узлы должны были развиваться за счет собственных ресурсов. Национальные сети других государств стали рассматриваться как отдельные домены, например UK — домен Великобритании, а DE — домен Германии. Тогда и появилось понятие Интернета как саморазвивающейся децентрализованной иерархической структуры. Если во времена ARPANET и NSFNET сеть финансировалась сверху вниз, то теперь она финансируется от периферии, снизу вверх — от конечных пользователей к владельцам опорных сетей.

Основы функционирования Интернета

В основе функционирования Интернета лежит пара протоколов TCP/IP. В этой паре протокол TCP (Transmission Control Protocol) выполняет функции транспортного уровня: он отвечает за то, как происходит передача данных. В свою очередь, протокол IP (Internet Protocol) — это адресный протокол, выполняющий функции сетевого уровня. Он определяет, куда именно происходит передача.

Согласно протоколу TCP, отправляемые данные «нарезаются» на небольшие пакеты, после чего каждый пакет маркируется таким образом, чтобы в нем было все необходимое для правильной сборки документа на компьютере получателя.

Для понимания сути протокола TCP можно представить игру в шахматы по переписке, когда двое участников разыгрывают одновременно десяток партий. Каждый ход записывается на отдельной открытке с указанием номера партии и номера хода. В этом случае между двумя партнерами через один и тот же почтовый

канал работает как бы десяток виртуальных соединений (по одному соединению на каждую партию). Два компьютера, связанные между собой одним физическим соединением, могут точно так же поддерживать одновременно множество TCP-соединений. Работая в Интернете, мы можем по одной физической линии связи принимать документы из Америки, Австралии и Европы практически одновременно. Пакеты каждого из документов поступают порознь, с разделением во времени, но прием всех документов происходит одновременно.

Теперь рассмотрим адресный протокол – IP. Он определяет способ записи адреса в Интернете для подключенных абонентских устройств. Такие устройства, обладающие уникальными адресами Интернета, называются *хостами* (как правило, это компьютеры, но не обязательно: хостами могут быть сетевые устройства, устройства мобильной связи, промышленные контроллеры и многие другие приборы). В свою очередь, уникальные интернет-адреса называются *IP-адресами*.

В настоящее время действуют две версии интернет-протокола: IPv4 и IPv6. Различаются они способами записи IP-адресов и, соответственно, методами их анализа. В версии IPv4 адрес хоста записывается 32 битами (четырьмя октетами по 8 бит в каждом, разделенными точками), например так: 195.38.46.11. Основным недостатком протокола IPv4 является ограниченность адресного пространства. С учетом того, что часть адресов отведена под служебные потребности, количество уникальных хостов не может превышать двух миллиардов. На заре Интернета эта величина казалась огромной, но для современного уровня развития информационного обмена этого совершенно недостаточно.

Адресное пространство протокола IPv6 в десятки раз шире, чем пространство IPv4, и в настоящее время может считаться неограниченным. Адрес хоста записывается 128 битами (восемь групп по четыре шестнадцатеричных числа, разделенные двоеточиями, например: 1234:5678:9abc:def0:0fed:cba9:8765:4321).

Службы Интернета

Когда говорят о работе в Интернете или об использовании Интернета, то на самом деле речь редко идет об Интернете в целом. Обычно имеется в виду одна из его многочисленных служб. В зависимости от конкретных целей и задач пользователи Сети используют те службы, которые им необходимы.

В простейшем понимании *сетевая служба* формируется парой программ, взаимодействующих между собой согласно определенным правилам, называемым протоколами. Одна из программ этой пары называется *сервером*, а вторая — *клиентом*. Соответственно, когда говорят о работе служб Интернета, речь идет о взаимодействии серверного оборудования и программного обеспечения и клиентского оборудования и программного обеспечения.

Разные службы имеют разные протоколы. Они называются *прикладными протоколами*. Их соблюдение обеспечивается и поддерживается работой специальных программ. Таким образом, чтобы воспользоваться какой-то из служб Интернета, необходимо установить на компьютере программу, способную работать по протоколу данной службы. Такие программы называют *клиентскими* или просто *клиентами*.