Глава 9

Налаживаем работу в сети: сетевые службы, клиенты, серверы, ресурсы. Защита при работе в сети

В этой главе вы найдете ответы на следующие вопросы:

- ***Для чего нужна сетевая операционная система?***
- ***Какие функции выполняют клиентские и серверные сетевые операционные системы?***
- ***Какие службы обеспечивают взаимодействие клиентских операционных систем в сетях Microsoft?***
- ***Какие существуют типы серверов?***
- ***Как строится система безопасности в современных сетевых ОС?***
- ***Какие меры защиты рекомендуется соблюдать при работе в сети?***

Итак, наша сеть заработала. Компьютеры объединены с помощью коммутаторов, точек доступа и, возможно, маршрутизаторов, везде установлен протокол TCP/IP и корректно настроены параметры IP.

Теперь нужно научиться работать в сети. Для этого нам потребуются *сетевые операционные системы* (ОС), с помощью которых пользователи смогут обмениваться информацией друг с другом, совместно работать с данными, использовать общие ресурсы и т. д.

Сетевые ОС можно разделить на *клиентские*, такие как Windows 2000 Professional, Windows XP Home Edition или Windows XP Professional, и *серверные*, например Windows Server 2003.

Основная функция клиентской сетевой ОС — предоставить пользователю удобный интерфейс для работы с сетевыми приложениями и службами, обеспечив при этом максимальную защиту компьютера и безопасность при доступе к данным и ресурсам. Серверы же выполняют сервисные функции, предоставляя свои данные и ресурсы для совместного использования, а также обслуживая различные клиентские запросы.

Какие же сервисы используются операционными системами для работы в сети? Начнем с клиентских операционных систем. Если посмотреть список

компонентов, используемых сетевыми подключениями ОС Windows 2000 Professional, то, кроме протокола TCP/IP, обеспечивающего межсетевые и транспортные функции, можно увидеть еще два сервиса: *Служба доступа к файлам и принтерам сетей Microsoft* и *Клиент для сетей Microsoft*. Эти две службы неразрывно связаны друг с другом: первая используется для предоставления каталогов и принтеров в общий доступ, вторая — для подключения к ним по сети.

В операционной системе Windows XP дополнительно предоставляется *Планировщик пакетов QoS* (Quality of Service) — служба, позволяющая *резервировать* некоторую часть общей полосы пропускания сетевого подключения, а затем *выделять* ее для таких приложений, где задержки недопустимы (например, при передаче по сети видеоизображения и речи при видеоконференцсвязи).

Таким образом, даже в клиентской ОС по умолчанию предусмотрена серверная служба доступа к файлам и принтерам. Эта служба позволяет в домашних или небольших офисных сетях обходиться без использования серверов (напомним: такие сети называются *одноранговыми*, или *рабочими группами*). Количество компьютеров в них обычно не превышает 10 (кстати, именно такое количество подключений является максимальным для клиентских ОС Windows). Компьютеры в одноранговых сетях обычно подключаются к одному концентратору или коммутатору, маршрутизаторы не используются. Чтобы обнаружить соседей, компьютеры применяют широковещательные сообщения, и никакие системы преобразования имен в IP-адреса при этом не требуются.

В крупных сетях без серверов уже не обойтись. Более того, чтобы удовлетворить постоянно возрастающим потребностям корпоративных пользователей, приходится постоянно повышать количество и

функциональность серверов, расширять их аппаратные возможности. Многие серверы приходится делать *специализированными* — предназначенными для поддержки конкретных служб или приложений. Другие, не очень сложные сервисы, наоборот, можно *объединять* (*консолидировать*) в рамках одного мощного аппаратного сервера.

Рассмотрим основные типы серверов.

- **Серверы, обеспечивающие работу в сети TCP/IP, или серверы сетевой инфраструктуры.** К ним относятся DHCP-, DNS- и WINS-серверы; обычно настройку работы в крупной сети начинают именно с них:

  - *DHCP-серверы* уже упоминались в прошлой главе. Они нужны, чтобы по запросу *DHCP-клиента* (компьютера, у которого в настройках протокола TCP/IP включен режим автоматического получения IP-адреса) выдать ему такие параметры, как уникальный IP-адрес и маска подсети. Кроме них, клиент может получать от DHCP-сервера ряд дополнительных параметров, важных для взаимодействия с другими сетями и удобной работы в сети: адрес основного шлюза, адреса DNS- и WINS-серверов, название домена, в который входит этот компьютер, и некоторые другие;

  - *DNS-серверы* выполняют очень важную функцию *преобразования (разрешения) имен узлов* (*host names*) *в соответствующие им IP-адреса*. Напомним: DNS (Domain Name System) расшифровывается как «система (служба) доменных имен». Служба DNS была реализована в Интернете в 1981 г., а с 2000 г. (с выходом ОС семейства Windows 2000) она стала основной службой преобразования имен в сетях Microsoft;

Под сервером в разных случаях может пониматься как собственно компьютер, так и установленное на нем специализированное программное обеспечение, либо весь этот программно-аппаратный комплекс в целом.

- *WINS-серверы* регистрируют в сети NetBIOS-имена компьютеров и их IP-адреса, а затем по запросу *WINS-клиентов* преобразуют эти имена в IP-адреса. Название WINS (Windows Internet Name Service) правильно переводится как «служба межсетевых имен Windows»; эта служба была разработана, чтобы обеспечить поддержку работы *NetBIOS- приложений* в маршрутизируемых сетях на базе протокола TCP/IP. Сейчас она по-прежнему используется, чтобы в сети корректно работали такие устаревшие ОС, как Windows 9*x* или Windows NT.

Напомним, что компьютеры для взаимодействия друг с другом используют IP-адреса. Человеку же с числовыми IP-адресами работать неудобно, поэтому при работе в сетях обычно используются словесные имена компьютеров. (Впрочем, в подавляющем большинстве приложений можно и непосредственно применять IP-адреса; иногда это удобный способ проверки работоспособности приложения, особенно если системы разрешения имен в данной сети не работают.)

Имена компьютеров при этом возможны двух типов:

- *имена узлов* — состоят из комбинаций букв, цифр и знака дефиса, разделенных точками. Это могут быть имена компьютеров как в Интернете (пример: `www.microsoft.com`), так и в локальной сети (`server1.domain.local`);
- *NetBIOS-имена* — «собственные» имена компьютеров, содержащие не более 15 любых символов, кроме точек (например, `SERVER1`).

➢ **Серверы файлов (файл-серверы)** нужны для хранения больших объемов данных и предоставления к ним доступа пользователей. Один файловый сервер может поддерживать одновременную работу сотен и

даже тысяч пользователей. Чтобы обеспечить сохранность информации, файл-серверы, как правило, оснащены отказоустойчивыми наборами (массивами) жестких дисков и системами резервного копирования на магнитную ленту или другой носитель.

- **Серверы печати (принт-серверы)** предназначены для обеспечения доступа пользователей к одному или нескольким общим принтерам. Они принимают по сети задания на печать, поступающие от пользовательских приложений, и управляют *очередями заданий на печать*, обычно обслуживая несколько печатающих устройств.

  Похожие функции выполняют и **факс-серверы**, обслуживающие клиентские задания на отправку факсов, но они, кроме того, отвечают за получение факсов и их доставку пользователям.

Файл-серверы и серверы печати — это одни из наиболее часто встречающихся типов серверов.

- **Серверы приложений** выполняют задачи обслуживания запросов пользователей на выборку или обработку какой-либо информации; их часто объединяют с **серверами баз данных**. Важно, что с серверами приложений и баз данных одновременно может работать большое число пользователей, причем выполнение клиентских запросов на специализированном многопроцессорном сервере производится намного быстрее, чем на компьютерах пользователей.

- **Серверы удаленного доступа** и **серверы VPN** (Virtual Private Network — «виртуальная частная сеть») обеспечивают удаленное подключение к локальной сети по модему или через Интернет. Это дает пользователям возможность работать с ресурсами локальной сети предприятия, офиса или учебного заведения из дома или из любого места, где есть подключение к Интернету, например из Интернет-кафе.

- **Терминальные серверы** предоставляют возможность работы с другими серверами через специальные программы — *терминальные клиенты*. С помощью этих программ администраторы, находясь вдалеке от локальной сети, оказываются как будто за консолью сервера и могут полностью управлять им, а пользователи могут удаленно работать с установленными на сервере приложениями.
- **Брандмауэры (межсетевые экраны)** используются при подключении к Интернету для защиты внутренней сети от проникновения или атаки злоумышленников на корпоративные серверы. **Прокси-серверы (серверы-посредники)** выполняют функции контроля доступа пользователей в Интернет и кэширования часто запрашиваемых веб-страниц (что позволяет снизить расходы на пользование Интернетом). Поскольку оба этих сервера предназначены для установки на компьютер, связывающий локальную сеть с Интернетом, их часто объединяют в единую программно-аппаратную систему.
- **Серверы электронной почты (почтовые серверы, mail-серверы)** обслуживают почтовые ящики пользователей в данной организации, обеспечивая подключения к ним *почтовых клиентов*, а также обрабатывают все входящие и исходящие сообщения. Их также можно использовать для ведения адресных книг, общих папок и систем электронного документооборота.
- **Веб- и FTP-серверы** предоставляют для внешних (а часто — и для внутренних) пользователей доступ к веб- и FTP-ресурсам, размещенным в данной сети.
- **Контроллеры домена** обеспечивают в сетях Microsoft работу служб *Активного каталога* (Active Directory) и поддерживают базу данных всех зарегистрированных в *домене* пользователей, компьютеров, групп и ресурсов. Наличие такой базы данных

позволяет администраторам централизованно управлять всеми сетевыми объектами и ресурсами. Пользователи же получают возможность входить в сеть с любого принадлежащего домену компьютера, а затем «прозрачно» (без ввода имени и пароля) подключаться к другим компьютерам и работать с их ресурсами.

Этот список далеко не полон, существуют и другие типы серверов. Однако перечисленные выше их разновидности можно найти практически в любой корпоративной сети.

Основы безопасности при работе в сетях

В те времена, когда компьютеры не были объединены в сети или подключены к Интернету, о безопасности данных можно было особенно не заботиться. Достаточно было обеспечить *физическую защиту* компьютера и контролировать доступ посторонних пользователей к устройствам записи (например, к дисководам).

После объединения компьютеров в сети все изменилось — без серьезной защиты теперь уже не обойтись, иначе и операционная система, и хранящиеся на компьютере или передаваемые по сети данные могут стать легкой добычей злоумышленников, причем так, что работающие на этом компьютере пользователи ничего не заметят. Поэтому далее мы изучим основные принципы, используемые при построении современных сетевых ОС, обсудим главные угрозы, представляющие опасность для компьютеров, пользователей и их данных, а также укажем простейшие правила обеспечения безопасности, которые обязательно следует соблюдать при работе в сети.

Принципы построения защищенных ОС:

- все современные ОС являются *многопользовательскими* — они рассчитаны на работу в системе (в том числе одновременную) нескольких пользователей;
- чтобы отличить одного пользователя от другого, применяются *учетные записи* (accounts) с уникальными *именами* и *паролями*;
- учетные записи различаются *уровнем полномочий* (*привилегий*, *прав*) — набором действий, которые обладатель данной учетной записи может выполнять в системе. Обычно учетные записи разделяют на *административные*, обладающие максимальными привилегиями, и *пользовательские*, набор полномочий для которых позволяет нормально работать в системе, но не разрешает выполнять какие-либо критичные с точки зрения безопасности данных операции, например форматировать разделы жесткого диска или менять настройки сети.

В обсуждаемых нами версиях ОС Windows дополнительно существуют учетные записи с уровнем прав, средним между административным и пользовательским (участники группы «Опытные пользователи»), а также обладающие минимальными полномочиями *гостевые учетные записи* (участники группы «Гости», включая встроенную учетную запись «Гость»).

Кроме того, существует два типа учетных записей — *локальные* из базы данных конкретного компьютера с ОС Windows, и *глобальные учетные записи в домене*, которые хранятся на контроллерах домена (подробнее о них будет сказано далее);

- для входа в компьютер обязательно нужно указать имя и пароль учетной записи, зарегистрированной в системе. Следует подчеркнуть, что понятие «вход в систему» подразумевает

не только непосредственный доступ, но и другие возможности работы с компьютером, например *сетевой* или *терминальный* вход, для которых также требуются пользовательские имя и пароль.

В операционных системах Windows допускается также сетевой вход без указания имени и пароля (*анонимный* вход); такие подключения используются при некоторых взаимодействиях в сетях Microsoft;

- после входа в систему (интерактивного, сетевого и т. д.) пользователь получает доступ к ресурсам того компьютера, в который он вошел (например, доступ к локальным файлам или каталогам). Уровень доступа при этом определяется *списком разрешений*, т. е. возможных действий, которые данный пользователь может осуществлять с защищенным объектом. Например, один пользователь может изменить или удалить файл, другой — только прочитать его, а третьему вообще будет отказано в доступе к этому файлу.

Рабочие группы и домены

Мы уже неоднократно упоминали *рабочие группы* и *домены*. Давайте разберем, чем принципиально отличаются эти две модели сетевого взаимодействия в сетях Microsoft.

Рабочая группа — это логическая группировка компьютеров, объединенных общим именем для облегчения навигации в пределах сети. Принципиально важно, что каждый компьютер в рабочей группе *равноправен* (т. е. сеть получается одноранговой) и *поддерживает собственную локальную базу данных учетных записей пользователей* (*Security Accounts Manager*, *SAM*).

Отсюда вытекает основная проблема, которая не позволяет использовать рабочие группы в крупных корпоративных сетях. Действительно, если вспомнить, что вход в защищенную систему является обязательным, а непосредственный и сетевой входы принципиально различаются (непосредственный контролируется локальным компьютером, а сетевой — удаленным), то, например, пользователю, вошедшему на компьютер `Comp1` под локальной учетной записью `User1`, будет отказано в доступе к принтеру, установленному на компьютере `Comp2`, поскольку в его локальной базе нет пользователя с именем `User1` (рис. 9.1). Таким образом, для обеспечения «прозрачного» взаимодействия в рабочей группе нужно *создавать одинаковые учетные записи с одинаковыми паролями на всех компьютерах*, где работают пользователи и расположены ресурсы.

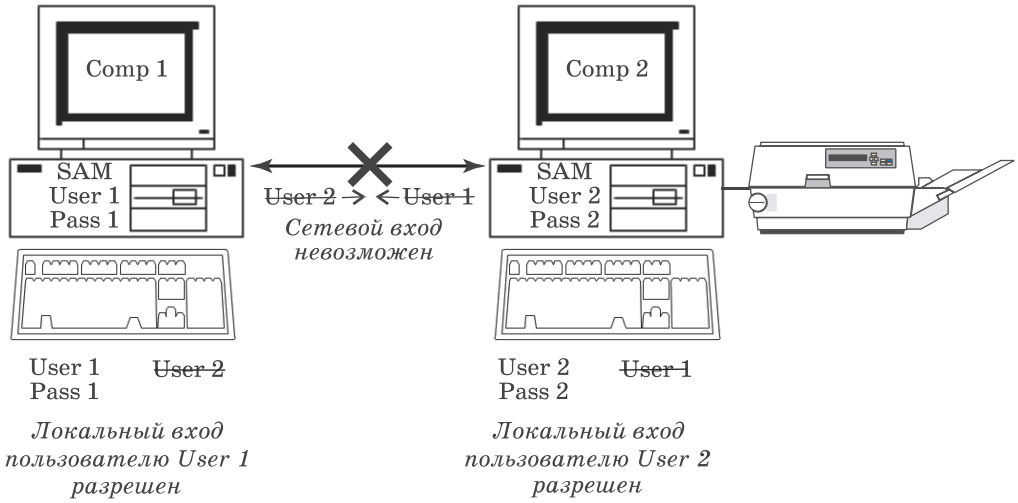

Рис. 9.1. Локальный и сетевой вход в систему в рамках рабочей группы

В ОС Windows XP Professional для рабочих групп предусмотрен специальный режим: «Использовать простой общий доступ к файлам», позволяющий обойти указанную проблему (данный режим включен по умолчанию). В этом случае подключение к любому сетевому компьютеру осуществляется от имени его локальной гостевой учетной записи, которая включается с помощью *Мастера настройки сети* (по умолчанию она отключена) и для которой настраивается нужный уровень доступа.

Для ОС Windows XP Home Edition этот способ сетевого взаимодействия является основным и отключить его нельзя (поэтому компьютеры с данной ОС невозможно сделать участниками домена).

Понятно, что управлять учетными записями и ресурсами в рабочей группе можно только при небольшом количестве компьютеров и пользователей. В крупных сетях следует применять домены.

Домен — это логическая группировка компьютеров, объединенных *общей базой данных пользователей и компьютеров, политикой безопасности и управления.*

Домены создаются на основе сетевых ОС Windows, а база данных, как мы уже говорили, поддерживается *контроллерами домена*. Важным в доменах является то, что все компьютеры здесь не сами осуществляют проверку пользователей при входе, а передоверяют эту процедуру контроллерам (рис. 9.2). Такая организация доступа позволяет легко осуществить однократную проверку пользователя при входе в сеть, а затем уже без проверки предоставлять ему доступ к ресурсам всех компьютеров домена.

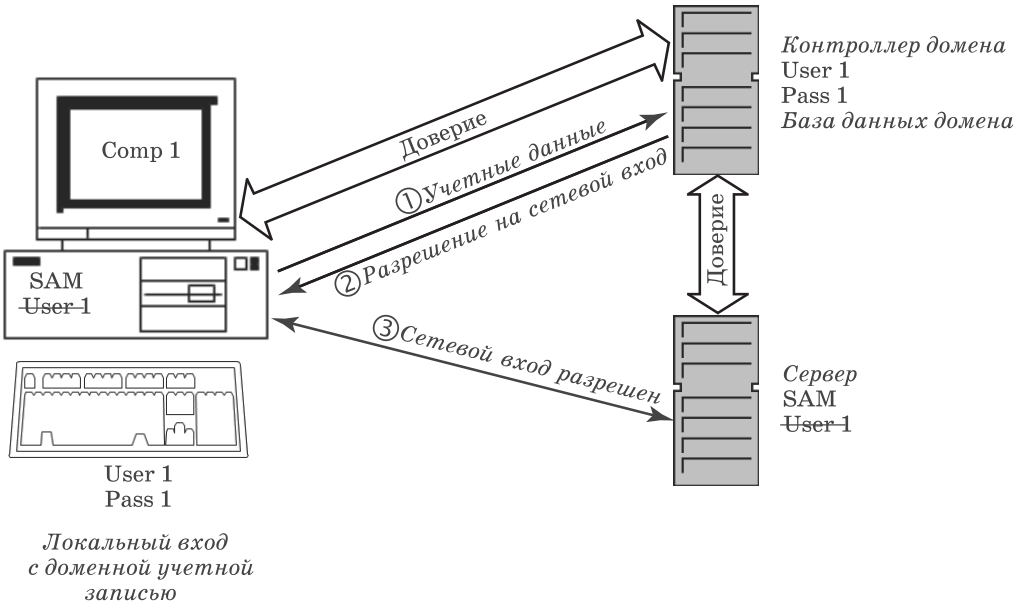

Рис. 9.2. Локальный и сетевой вход в домене

Основные угрозы при работе в сети

Угроз, поджидающих пользователей при подключении компьютера к сети, довольно много. Мы приведем только основные из них:

- *«взлом» компьютера* обычно производится с целью захвата контроля над операционной системой и получения доступа к данным;
- *повреждение системы* чаще всего организуется, чтобы нарушить работоспособность (вызвать отказ в обслуживании — «Denial of Service») каких-либо сервисов или компьютера (чаще сервера) целиком, а иногда — даже всей сетевой инфраструктуры организации;

«Троянские» программы получили свое название «в честь» знаменитого «троянского коня», придуманного хитроумным Одиссеем, чтобы захватить Трою. Типичная «троянская» программа обычно «маскируется» под какую-либо полезную утилиту (или может быть спрятана в какой-либо программе), а если пользователь по незнанию запустит ее на выполнение, такая программа начинает контролировать компьютер, открывая создателю «троянской программы» доступ к данным (так называемый «backdoor» — «черный ход»), похищая и пересылая ему набираемые с клавиатуры пароли и т. п.

- *кража данных* из-за неправильно установленных прав доступа, при передаче данных или «взломе» системы позволяет получить доступ к защищаемой, часто — конфиденциальной информации со всеми вытекающими отсюда неприятными для владельца этих данных последствиями;
- *уничтожение данных* имеет целью нарушить или даже парализовать работу систем, компьютеров, серверов или всей организации.

Атаки на компьютеры или серверы, вирусы, «черви», шпионские и «троянские» программы — все это злонамеренное ПО пишется для того, чтобы осуществить в той или иной степени перечисленные выше угрозы.

Основные меры безопасности при работе в сети довольно просты. Их можно сформулировать в виде следующего набора правил:

- отключайте компьютер, когда вы им не пользуетесь. Как любят говорить эксперты по компьютерной безопасности, «самым защищенным является выключенный компьютер, хранящийся в банковском сейфе»;
- своевременно обновляйте операционную систему. В любой ОС периодически обнаруживаются так называемые «*уязвимости*», снижающие защищенность вашего компьютера. Наличие уязвимостей нужно внимательно отслеживать (в том числе читая «компьютерную» прессу или информацию в Интернете), чтобы вовремя предпринимать меры для их устранения.

Для ОС Windows корпорацией Microsoft создан специальный веб-узел Windows Update, обратившись к которому (например, с помощью программы WUPDMGR.EXE или команды **Windows Update** в меню **Пуск**), нетрудно просмотреть и скачать список *обновлений*, рекомендуемых для вашего компьютера;

- используйте ограниченный набор хорошо проверенных приложений, не устанавливайте сами и не разрешайте другим устанавливать на ваш компьютер программы, взятые из непроверенных источников (особенно из Интернета). Если приложение больше не нужно, удалите его;
- без необходимости не предоставляйте ресурсы своего компьютера в общий доступ. Если же это все-таки потребовалось, обязательно настройте минимально необходимый уровень доступа к ресурсу только для зарегистрированных учетных записей;
- установите (или включите) на компьютере *персональный межсетевой экран* (*брандмауэр*). Если речь идет о корпоративных сетях, установите брандмауэры как на маршрутизаторах, соединяющих вашу локальную сеть с Интернетом, так и на всех компьютерах сети;
- обязательно установите на компьютер специализированное антивирусное и «антишпионское» программное обеспечение. Настройте его на автоматическое получение обновлений как минимум один раз в неделю (лучше — ежедневно или даже несколько раз в день);
- даже если вы единственный владелец компьютера, для обычной работы применяйте *пользовательскую учетную запись*: в этом случае повреждение системы, например, при заражении вирусом, будет неизмеримо меньше, чем если бы вы работали с правами администратора. Для всех учетных записей, особенно административных, установите и запомните сложные пароли.

Сложным считается пароль, содержащий случайную комбинацию букв, цифр и специальных символов, например `jxg1rg$N`. Разумеется, пароль не

должен совпадать с именем вашей учетной записи. В операционных системах Windows сложный пароль можно *сгенерировать* автоматически, используя команду NET USER с ключом /RANDOM, например:

```
NET USER Имя_Пользователя /RANDOM
```

Пароль в виде случайной последовательности символов нелегко запомнить, поэтому часто используют следующую технику — пароль набирается в английской раскладке русскими буквами. Например, слово «Пароль» тогда будет выглядеть как «Gfhjkm». Однако этот способ следует применять с осторожностью — взломщики давно имеют целые словари подобным образом преобразованных слов, так что желательно вставлять в такие пароли специальные символы и цифры.

Пароли для доступа в различные системы должны быть разными. Недопустимо использовать один и тот же пароль для администрирования вашего компьютера и для входа, например, на игровой веб-сайт;

«Фишинг» («рыбная ловля») — так называется распространенный сегодня вид мошенничества в Интернете. Злоумышленники создают сайты, внешне похожие на сайты Интернет-магазинов, банков и пр., а затем «заманивают» на них посетителей (например, с помощью рекламных баннеров) и предлагают «подтвердить свои персональные данные». Иногда злоумышленники с той же целью рассылают электронные письма якобы от имени администрации почтового сервера с просьбой «подтвердить пароль доступа к почтовому ящику».

- при работе с электронной почтой никогда сразу не открывайте вложения, особенно полученные от неизвестных отправителей. Сохраните вложение на диск, проверьте его антивирусной программой и только затем откройте. Если есть такая возможность, включите в вашей почтовой программе защиту от потенциально опасного содержимого и отключите поддержку HTML;
- при работе с веб-сайтами соблюдайте меры разумной предосторожности: старайтесь избегать регистрации, не передавайте никому персональные сведения о себе и внимательно работайте с Интернет-магазинами и другими службами, где применяются онлайновые способы оплаты с помощью кредитных карт или систем типа WebMoney, Яндекс-Деньги и т. д.

При резервном копировании полезно использовать утилиты для создания «образов» жесткого диска (такие, как Norton Ghost). Резервную копию можно снять с «системного» жесткого диска после правильной установки на него всех требуемых программ и антивирусной проверки и хранить ее на другом жестком диске (сетевом или съемном), чтобы в случае повреждения системы быстро восстановить ее работоспособность.

При проведении оплаты убедитесь, что соединение защищено шифрованием с помощью технологии *Secure Sockets Layer* (*SSL*) — в этом случае адресная строка обязательно должна начинаться с «`https://`»;

- перечисленные выше меры лишь повышают общую защищенность системы и данных, но не дают никакой гарантии от их повреждения или даже полной потери. Поэтому обязательно следует создавать *резервные копии* системы и данных на съемном жестком диске или на DVD-RW — это позволит вам легко восстановить их в случае утери. При этом одну копию имеет смысл хранить вне дома, например, в сейфе;
- исключительно важную роль играет обучение всех пользователей основам безопасной работы в сетях — как в домашних, так и в корпоративных, — ведь нарушение правил одним пользователем ставит под угрозу всю систему защиты.

Итак, для работы в сети нужны сетевые операционные системы, которые принято делить на клиентские и серверные. Клиентские ОС отличаются небольшим набором служб, но включают в себя спектр сетевых приложений. Серверные системы бывают различных типов и предназначены для обслуживания тех или иных запросов сетевых клиентов.

Для организации работы в сетях Microsoft применяются две модели: рабочие группы, используемые при небольшом числе компьютеров, и домены, позволяющие легко объединять большое число пользователей, рабочих станций и серверов.

Все сетевые ОС и хранящиеся на компьютерах данные должны быть надежно защищены, причем желательно, чтобы применяемая система безопасности была многоуровневой.

Вопросы и задания

1. Для чего нужны сетевые операционные системы? Чем они отличаются от «несетевых»? Какие возможны типы сетевых операционных систем?
2. Чем различаются клиентские и серверные сетевые операционные системы?
3. Какие сетевые сервисы и службы предоставляются в Windows 2000 и XP?
4. Какие возможны виды серверов? Каково их назначение? Чем они различаются?
5. В чем заключается проблема безопасности при работе в сети? Чем она вызвана?
6. Каковы принципы организации работы пользователей в защищенных ОС?
7. В чем заключается *авторизация* (идентификация) пользователей? Как она реализуется?
8. Какие возможны виды учетных записей? Какая информация входит в учетную запись? Какие права доступа могут обеспечиваться для пользователя учетной записи в ОС Windows?
9. Что такое рабочая группа? Что такое домен? В чем заключается их основное различие?
10. Каковы основные угрозы при работе в сети? Каковы, по вашему мнению, основные причины (мотивы), побуждающие злоумышленников осуществлять подобные действия?
11. Каковы основные правила (меры) безопасности при работе в сети?
12. Какие дополнительные меры безопасности, по вашему мнению, необходимы при работе в сети (в частности, в Интернете) несовершеннолетних? Как вы организовали бы работу с Интернетом для своего ребенка на своем домашнем компьютере? в школьном компьютерном классе?