ЛЕГКИЙ СТАРТ

Д. Донцов

Как защитить компьютер
от ошибок, вирусов, хакеров

ПИТЕР®

Москва · Санкт-Петербург · Нижний Новгород · Воронеж
Новосибирск · Ростов-на-Дону · Екатеринбург · Самара
Киев · Харьков · Минск
2007

ББК 32.973.23-07
УДК 004.382.7
Д67

Донцов Д.
Д67 Как защитить компьютер от ошибок, вирусов, хакеров. — СПб.: Питер, 2007. — 144 с.: ил. — (Серия «Легкий старт»).

ISBN 5-469-01345-6

Бытует мнение, что компьютеру можно доверить все: личную переписку, пин-код банковской карты, электронные документы. На самом деле компьютер сможет надежно хранить ваши данные, только если вы сами позаботитесь об их защите. Эта книга поможет вам в этом. Прочитав ее, вы узнаете, как защититься от вирусов, шпионских модулей и прочих вредоносных программ, как не попасться на крючок интернет-мошенников и как спрятать конфиденциальные данные от чужих глаз. Книга расскажет вам о том, что делать, если вы случайно удалили нужный файл или неосторожными действиями повредили Windows. Немало внимания уделено типичным сбоям ПК и способам их устранения. Можете быть уверены: освоив эту книгу, вы с легкостью справитесь с любой проблемой, которая потенциально может возникнуть с вашим компьютером.

ББК 32.973.23-07
УДК 004.382.7

ISBN 5-469-01345-6

Оглавление

Введение

Ни для кого не секрет, что в настоящее время компьютер прочно и надолго вошел в нашу повседневную жизнь. Возможности компьютера используются на работе, при проведении досуга, в быту и других сферах жизнедеятельности человека. Количество информации, которую мы доверяем своему «электронному другу», с каждым днем растет. Поэтому рано или поздно каждый пользователь задается вопросом: «Как обеспечить надежную сохранность данных?»

В большинстве случаев такой вопрос возникает лишь после того, как случилась определенная неприятность. Следовательно, чаще всего пользователи задумываются о мерах по обеспечению сохранности данных только после их полной или частичной потери (или при возникновении ситуации, когда потери данных удалось избежать только чудом). Чтобы не попадать в подобные переделки, достаточно соблюдать несложные правила безопасности.

В этой книге мы рассмотрим, как можно избежать непредвиденных потерь важной информации.

Как известно, компьютерные технологии развиваются с каждым днем и новые достижения могут использоваться не только во благо пользователей. Программы, разработанные со злым умыслом, способны причинить немалый ущерб. Поэтому, кроме рекомендаций по избежанию потерь данных, в книге рассмотрены приемы и способы восстановления потерянной информации.

От издательства

Ваши замечания, предложения и вопросы отправляйте по адресу электронной почты gurski@minsk.piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На сайте издательства http://www.piter.com вы найдете подробную информацию о наших книгах.

1. Защищенность компьютера: мифы и реальность

Защищенность компьютера (а следовательно, и хранящейся в нем информации) зависит от многих индивидуальных факторов: специфики его использования, загруженности, наличия опыта работы у пользователя и др. Однако существуют общие причины, вызывающие потерю данных. С наиболее распространенными из них вы познакомитесь в этой главе.

Однако прежде всего напомню основные правила эксплуатации персонального компьютера, соблюдение которых не только продлевает срок службы устройства, но и имеет важное значение с точки зрения сохранности информации.

Основные правила эксплуатации компьютера

Рассмотренные в данном подразделе правила придуманы не сегодня и не вчера; они формировались на основе многолетнего опыта работы с компьютерами. Большинству пользователей эти положения наверняка знакомы, однако соблюдают их далеко не все. Итак, при эксплуатации компьютера необходимо придерживаться следующих рекомендаций.

- Сведите к минимуму возможность попадания пыли в системный блок. Пыль может вызывать перегрев компонентов компьютера, периодическое исчезновение контактов и др. Не рекомендуется устанавливать системный блок на пол, поскольку именно там обычно скапливается пыль. Периодически, хотя бы раз в год, выполняйте профилактическую очистку компьютера: удаляйте накопившуюся пыль с его компонентов.
- Следите за температурным режимом работы компонентов компьютера. Все установленные вентиляторы и кулеры долж-

ны функционировать, а при поломке такое устройство необходимо оперативно отремонтировать или заменить. Для слежения за температурным режимом удобно использовать специальные утилиты, которые можно найти в Интернете.

- Не следует устанавливать компьютер в местах, которые могут вызвать его преждевременный перегрев (например, в зоне попадания прямых солнечных лучей).
- Если компьютер какое-то время находился на холоде (при температуре ниже 0 °С), то перед включением оставьте его на 2–3 часа в теплом помещении.
- Необходимо обеспечить нормальное электропитание компьютера. Качество отечественной электроэнергии оставляет желать лучшего (об этом более подробно рассказано в подразд. «Проблемы с электропитанием»), поэтому следует защитить компьютер от возможных скачков напряжения, внезапного отключения электроэнергии и т. п. Для этого необходимо использовать сетевой фильтр, а лучше всего — источник бесперебойного питания.
- Не стоит самостоятельно экспериментировать с внутренним устройством компьютера. Если вам нужно внести какие-либо изменения в его конфигурацию, лучше доверить эту процедуру специалисту (или получить у него подробную консультацию). Например, несложная, на первый взгляд, операция — добавление оперативной памяти — может не только не привести к ожидаемым результатам (в частности, к увеличению быстродействия), но и вызвать неправильную работу некоторых приложений, что может закончиться большими неприятностями. Причина этого может быть в том, что выбранная память просто несовместима с некоторым другим оборудованием, установленным на компьютере.
- Обязательно установите хорошую антивирусную программу. Даже если вы не работаете с Интернетом, существует риск подхватить вирус с дискеты, компакт-диска, из локальной сети и др. Периодически проводите полное сканирование компьютера на наличие вирусов с помощью антивирусной программы.
- При работе в Интернете настоятельно рекомендуется использовать брандмауэр. Стандартный интернет-обозреватель

Internet Explorer имеет встроенный брандмауэр. Однако опытные хакеры давно научились обходить его, поэтому рекомендуется использовать другую защиту: например, все большую популярность завоевывает программа ZoneAlarm. Она имеет как платную, так и бесплатную версии; каждую из них можно скачать в Интернете.

- Каждый сеанс работы необходимо завершать с использованием штатной функции завершения работы операционной системы.

Причины потери информации

К основным причинам, приводящим к потере хранящейся в компьютере информации, можно отнести следующие:

- нестабильная работа операционной системы;
- нестабильное электропитание (в том числе внезапное отключение электроэнергии);
- действия вирусов и других вредоносных программ;
- неквалифицированные действия пользователей (в частности, внесение некорректных изменений в системный реестр, безграмотное редактирование системных файлов и т. п.);
- повреждение жесткого диска.

Рассмотрим каждую из перечисленных причин подробнее, а также то, каким образом можно предупредить ее появление или избежать негативных последствий, если она уже каким-то образом проявила себя.

Нестабильная работа операционной системы

Нестабильность в работе операционной системы обычно проявляется после ее продолжительного использования. При этом могут возникать различного рода сбои, скорость работы системы может существенно уменьшиться, а место, занимаемое системной папкой на жестком диске, — значительно увеличиться. В итоге в какой-то момент система может вообще не загрузиться.

Подобная ситуация возникает, как правило, в результате того, что в операционной системе со временем накапливаются различные вспомогательные файлы, библиотеки и настройки (например, в результате инсталляции программ), которые могут начать конфлик-

товать как друг с другом, так и с операционной системой. Несмотря на то что большинство современных программ имеют встроенные режимы деинсталляции, программа не всегда удаляется корректно и бесследно для операционной системы (что уж говорить о приложениях, которые не имеют штатных средств для удаления). В результате остаются «хвосты», которые не только засоряют системный реестр, но и могут дополнительно отвлекать ресурсы оперативной памяти.

Чтобы избежать подобных неприятностей, рекомендуется периодически очищать системный реестр. Разумеется, это делается не вручную: для очистки реестра следует применять специально разработанные программы и утилиты, которых в настоящее время существует великое множество. Они могут быть платными, условно платными и бесплатными. Дистрибутив или исполняемый файл большинства таких программ вы легко найдете в Интернете.

Рассмотрим популярную программу, которую удобно использовать для очистки реестра, — менеджер реестра Reg Organizer. На момент написания книги вышла версия Reg Organizer 3.1, однако она является платной (существует также бесплатная триал-версия, рассчитанная на работу в течение 30 дней). Рассмотрим программу на примере версии 2.5, которую вы можете бесплатно скачать из Интернета.

Reg Organizer представляет собой многофункциональную утилиту, предназначенную для работы с системным реестром. В этой книге не будем подробно рассматривать все ее функциональные возможности, а остановимся лишь на имеющих непосредственное отношение к рассматриваемой проблеме.

Интерфейс программы Reg Organizer в режиме очистки реестра представлен на рис. 1.1.

В программе предусмотрено использование следующих режимов:

- редактирования реестра;
- очистки реестра;
- редактирования файлов;
- поиска и замены в реестре;
- деинсталляции программ.

Требуемый режим можно включить, выбрав соответствующий пункт в меню Режим. Интерфейс, изображенный на рис. 1.1, откроется после выполнения команды Режим ▸ Режим чистки реестра.

Рис. 1.1. Менеджер реестра Reg Organizer

Перед тем как приступить к очистке реестра, рекомендуется просмотреть и при необходимости отредактировать некоторые параметры работы программы. Для этого следует нажать на панели инструментов окна программы кнопку Установки и в открывшемся окне перейти на вкладку Поиск ссылок на несуществующие файлы. Здесь определяют разделы реестра, которые будут сканироваться, порядок удаления неверных записей и другие параметры. Настройки параметров на данной вкладке просты и интуитивно понятны, поэтому подробно останавливаться на этом не будем.

Чтобы приступить к очистке реестра, следует нажать кнопку Чистка реестра. В результате откроется окно, изображенное на рис. 1.2.

В данном окне в поле Что искать определяют объекты поиска. Для выбора объектов предназначены следующие флажки:

- Неверные расширения;
- Ссылки на несуществующие файлы и папки;
- Пустые ключи деинсталляторов;

- Неверные ссылки на DLL;
- Неверные ссылки на шрифты;
- Неверную деинсталляционную информацию;
- Неверная информация CLSID.

В поле Просматривать ключи аналогичным образом выбирают параметры реестра, которые следует сканировать. Следует учитывать, что выбор параметров возможен, только если в области Что искать установлен флажок Ссылки на несуществующие файлы и папки (то есть выбор параметров имеет значение только для режима Ссылки на несуществующие файлы и папки). По умолчанию установлены флажки тех параметров, которые выбраны на вкладке Поиск ссылок на несуществующие файлы окна настройки программы.

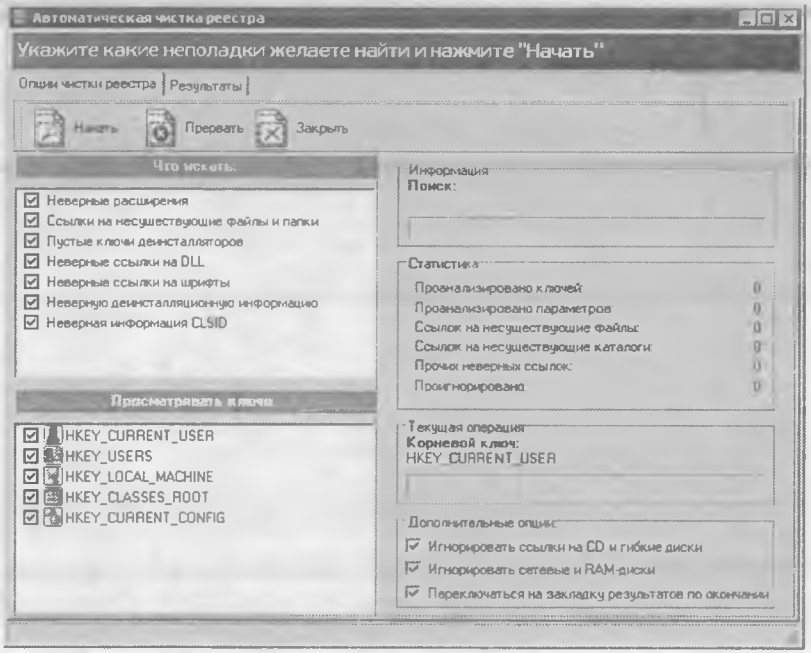

Рис. 1.2. Очистка реестра

Справа внизу окна в области Дополнительные опции можно при необходимости задать дополнительные параметры сканирования. Для этого предназначены такие флажки:

- Игнорировать ссылки на CD и гибкие диски;
- Игнорировать сетевые и RAM-диски;
- Переключаться на закладку результатов по окончании (если установлен данный флажок, то в окне, изображенном на рис. 1.2, после окончания сканирования автоматически откроется вкладка Результаты).

Чтобы запустить процесс сканирования реестра, нажмите кнопку Начать, которая расположена в верхней части окна.

Информация о текущем состоянии сканирования динамически отображается в соответствующих информационных полях в правой части окна.

Чтобы остановить сканирование, нужно воспользоваться кнопкой Прервать. С помощью кнопки Закрыть можно выйти из данного режима.

Результаты проверки системного реестра представлены на вкладке Результаты (рис. 1.3).

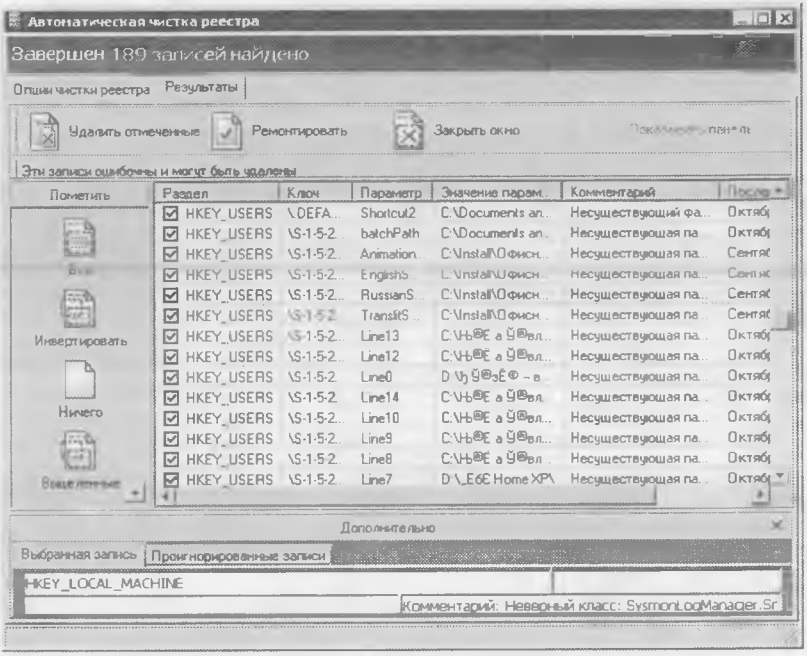

Рис. 1.3. Результаты проверки системного реестра

Здесь отображается список всех обнаруженных в реестре ошибочных, лишних и устаревших записей, которые можно удалить. Для каждой позиции списка в соответствующих столбцах отображаются разделы и параметры реестра, значение параметра, комментарий (тип записи) и дата последнего изменения.

С помощью кнопки Ремонтировать можно перейти в режим поиска объектов, на которые указывают неверные ссылки. Однако этот режим позволяет исправить только ссылки на несуществующие файлы (в значениях параметров) и неверные ссылки на шрифты; прочие виды ссылок будут проигнорированы.

При нажатии кнопки Удалить отмеченные из системного реестра будут удалены все записи, отмеченные в списке флажками. По умолчанию отмечены все позиции списка, но при необходимости можно снять определенные флажки, что позволит удалить ошибочные записи выборочно.

В левой части окна, в области Пометить, находятся несколько кнопок. С помощью кнопки Все можно быстро отметить флажками одновременно все позиции списка. Кнопка Инвертировать действует следующим образом: если все флажки установлены, то нажатием данной кнопки можно снять их, если флажки сняты — установить. При нажатии кнопки Ничего все флажки будут сняты. Кнопка Выделенные используется для пометки выделенных пунктов списка.

Если на любом пункте списка щелкнуть правой кнопкой мыши, то откроется контекстное меню, содержащее следующие команды.

- При выборе пункта Открыть ключ в редакторе реестра данная позиция списка откроется в режиме редактирования реестра.
- С помощью пункта Добавить элемент в список исключений выбранную позицию можно занести в список исключений. Записи, добавленные в список исключений, при последующих проверках системного реестра за ошибку не принимаются.
- При выборе пункта Добавить все выбранные элементы в список исключений все отмеченные позиции будут добавлены в список исключений.
- Команда Список исключений предназначена для перехода в режим работы со списком исключений.
- Команда Сохранить список как используется для сохранения списка ошибочных записей в отдельном текстовом файле. Данную возможность целесообразно использовать, например, если

необходимо подробно проанализировать содержимое списка, но в данный момент это по каким-то причинам невозможно. При выборе этого пункта на экране появится окно Сохранить как, в котором по обычным правилам Windows указывают путь для сохранения и имя файла.

По умолчанию Reg Organizer автоматически создает резервную копию удаляемых из реестра ошибочных данных. Для работы с резервными копиями (восстановления, удаления и других действий) предназначена команда главного меню Команды ▸ Резервные копии.

Помимо очистки системного реестра, программа Reg Organizer позволяет выполнять файловую очистку системы. Для перехода в соответствующий режим в окне, изображенном на рис. 1.1, необходимо нажать кнопку Чистка файлов. В результате на экране появится окно, показанное на рис. 1.4.

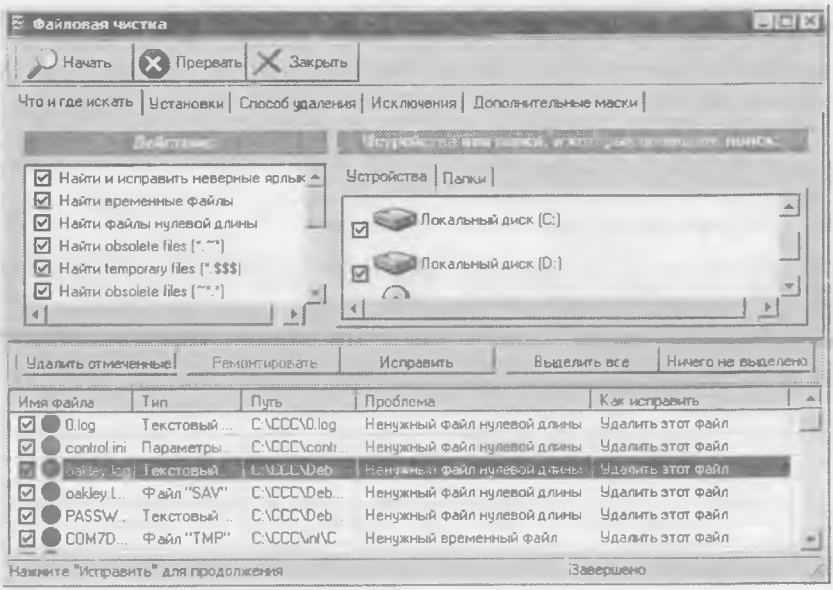

Рис. 1.4. Режим очистки файлов

В верхней части данного окна настраивают параметры файловой очистки, а в нижней отображается список записей, обнаруженных в соответствии с настроенными параметрами.

Верхняя часть окна содержит несколько вкладок. Кратко остановимся на каждой из них.

На вкладке Что и где искать в области Действие путем установки соответствующих флажков выбирают типы объектов, которые нужно найти (временные файлы, файлы нулевой длины и т. п.).

В области Устройства или папки, в которых проводить поиск задают диски и папки компьютера, в которых будет проведен поиск.

При этом диски выбирают с помощью соответствующих флажков на вкладке Устройства, а список папок формируют на вкладке Папки.

На вкладке Установки окна Файловая чистка следует настроить процесс сканирования. Для этого предназначены такие флажки:

- Игнорировать ссылки на CD-ROM;
- Игнорировать ссылки на гибкие и иные отсоединяемые диски;
- Игнорировать ссылки на сетевые и RAM-диски;
- Пропускать системные файлы и папки;
- Пропускать скрытые файлы и папки.

По умолчанию установлены все флажки, кроме Пропускать скрытые файлы и папки. Настоятельно рекомендую установить и этот флажок.

На вкладке Способ удаления определяют, каким образом должны удаляться найденные объекты. Переключатель может принимать следующие положения:

- Стирать с диска;
- Удалять в Корзину;
- Перемещать в папку (при выборе данного варианта следует указать путь к папке, в которую найденные объекты должны быть помещены при удалении).

На вкладке Исключения формируется список исключений. Включенные в этот список объекты будут проигнорированы при сканировании.

На вкладке Дополнительные маски можно при необходимости настроить произвольные маски для поиска.

Чтобы запустить процесс сканирования в соответствии с настроенными параметрами, следует нажать кнопку Начать, которая расположена в верхней части окна Файловая чистка. Для остановки поиска предназначена кнопка Прервать.

После окончания сканирования список найденных файлов появляется в нижней части окна (см. рис. 1.4). Для каждого файла в соответствующих столбцах отображается следующая информация:

- имя найденного файла;
- тип файла (текстовый, временный и т. п.);
- полный путь к файлу;
- краткое описание проблемы (почему файл считается ненужным);
- рекомендуемый способ исправления; после исправления в данном столбце появляется состояние (статус) файла (например, Удален).

Чтобы удалить файлы из списка, нужно пометить их с помощью соответствующих флажков, после чего нажать кнопку Удалить отмеченные. Для быстрой пометки всех позиций списка предназначена кнопка Выделить все, для снятия всех флажков следует воспользоваться кнопкой Ничего не выделено. Нажатием кнопки Исправить можно исправить все записи в соответствии со способом, рекомендованным в столбце Как исправить.

Рассмотренным способом можно быстро очистить систему от ненужных и неиспользуемых файлов.

Проблемы с электропитанием

Любой пользователь компьютера должен учитывать, что отечественная электроэнергия отличается совсем невысоким качеством. Данная проблема касается не только Российской Федерации, но и практически всех стран СНГ. На первый взгляд это незаметно, и многие могут задать вопрос: «Неужели мы постоянно пользуемся некачественной электроэнергией?»

Дело в том, что персональный компьютер представляет собой гораздо более тонкий механизм, чем остальная техника. Перепады напряжения в электрической сети, не имеющие никаких последствий, например, для холодильника или телевизора, могут в то же время привести к серьезной поломке компьютера. Причины таких перепадов могут быть самые разные: от природных катаклизмов (например, грозы) до внезапно включенной соседом электродрели. Кроме того, как уже отмечалось, отечественная электроэнергия может в любой момент преподнести вам неприятный сюрприз без всяких видимых причин.

Следует учесть и то, что электропроводка в подавляющем большинстве домов (опять же речь идет о территории СНГ) безнадежно устарела и морально, и физически. Заземление имеется только в новых домах, построенных за последние 10–15 лет; в большинстве зданий такая «роскошь» не предусмотрена.

Кроме этого, можно отметить еще одну неприятную особенность, которая также проявляется в основном в домах советской постройки. Электрические сети, проложенные в таких домах, не рассчитаны на современную нагрузку — ведь во время их строительства у людей не было такого количества бытовой техники, как сейчас. Если раньше в стандартном доме было, может, три-пять стиральных машин на подъезд, то сейчас они есть почти в каждой квартире. Раньше нормой считался один телевизор на семью, а сейчас многие имеют по два, а то и по три телевизора. Кроме того, многие сегодня имеют электрочайники, обогреватели, микроволновые печи и т. д. Представьте, какая нагрузка ложится на сеть, проложенную в 60–80 годах прошлого века! Поэтому многим, наверное, известна такая ситуация: сосед включил электрочайник (или обогреватель) и по всему «стояку» в подъезде отключился свет.

Разумеется, подобные «электрические» приключения не могут проходить для персонального компьютера бесследно, а в некоторых случаях они просто губительны. Если в результате проблем с электропитанием оказалась утеряна только информация, введенная или измененная во время последнего сеанса работы, — это можно считать удачей. Гораздо более неприятно, когда следствием перепадов напряжения или иных «катаклизмов» является выход из строя оборудования (материнской платы, жесткого диска, блока питания и др.). Это чревато не только финансовыми затратами на ремонт компьютера, но и полной потерей хранящейся в нем информации (что в большинстве случаев более ощутимо).

Каким образом можно защититься от проблем, вызываемых нестабильным или некачественным электропитанием?

В первую очередь отмечу, что ни в коем случае нельзя включать компьютер в обычную электрическую розетку — это верный способ быстро вывести его из строя. Как минимум необходимо использовать сетевой фильтр. Иногда он продается в комплекте с компьютером, но чаще это устройство приходится приобретать отдельно. Сетевой фильтр внешне представляет собой обычный удлинитель-«тройник» (правда, имеющий не три, а четыре или пять гнезд), снабженный

2–2760

тумблером-выключателем. Однако такой фильтр способен защитить компьютер только от несущественных перепадов напряжения и совершенно бесполезен при внезапном отключении электроэнергии.

Для более надежной защиты компьютера от сбоев в электропитании рекомендуется использовать специальное устройство — источник бесперебойного питания (ИБП). Характерной особенностью ИБП является то, что компьютер питается именно от него, а не непосредственно от сети. Иначе говоря, источник бесперебойного питания — это своеобразный буфер между электрической сетью и компьютером. В его состав, помимо других компонентов, входит аккумуляторная батарея, средний срок службы которой — от трех до пяти лет. Эта батарея позволяет корректно завершить работу компьютера и спокойно выключить его даже после внезапного отключения электроэнергии. Перед первым использованием такую батарею нужно заряжать примерно 4–6 часов; подробно об этом написано в руководстве пользователя.

Кроме этого, источник бесперебойного питания «сглаживает» любые перепады напряжения в сети, тем самым защищая персональный компьютер от связанных с этим поломок. Следует отметить, что многие ИБП защищают также модем от перепадов напряжения в телефонной сети. В таких устройствах предусмотрены специальные гнезда для подключения провода модемной связи. В данном случае ИБП выступает как «буфер» между модемом и телефонной линией.

В настоящее время на рынке представлено множество различных источников бесперебойного питания — как отечественного производства, так и импортных. При выборе следует руководствоваться в первую очередь техническими характеристиками устройства, а именно совместимостью с вашим компьютером. Не рекомендуется приобретать источник бесперебойного питания с рук или на рынке.

Действия вирусов и других опасных программ

Наверное, сегодня нет ни одного пользователя, который не слышал бы о различных вредоносных программах. В первую очередь к ним относятся так называемые компьютерные вирусы. Что же представляют собой вирусы и каковы могут быть последствия их действий?

Компьютерный вирус — это вредоносная программа, проникающая в компьютер и выполняющая в нем определенные действия без

ведома пользователя. Заразиться вирусом можно где угодно — в Интернете, в локальной сети, с дискеты или компакт-диска и др.

Традиционно наиболее «заразными» местами считаются развлекательные сайты «пикантной» направленности (проще говоря, порносайты) и компьютеры, установленные в общественных местах. К последним относятся, например, компьютеры в аудиториях вузов и интернет-кафе: за день таким компьютером пользуются десятки посетителей, и каждый работает со своей дискетой, на которой может быть записано неизвестно что.

Наряду с относительно безвредными вирусами существуют и настоящие «злодеи», способные не только уничтожить хранящуюся в компьютере информацию, но и вывести из строя его аппаратную часть. Однако сейчас подробно останавливаться на вирусах и защите от них не будем, поскольку данные вопросы подробно рассмотрены далее, в соответствующем разделе.

Неквалифицированные действия пользователей

Наверное, ни один вирус и перепад напряжения в сети не могут причинить такой ущерб компьютеру и хранящейся в нем информации, какой могут вызвать неквалифицированные действия пользователя. Такие действия можно условно разделить на три группы:

- редактирование системного реестра;
- редактирование системных и загрузочных файлов;
- попытка самостоятельно починить компьютер (или изменить параметры его работы) путем проникновения внутрь системного блока (иначе говоря, различные эксперименты с «железом»).

Реестр Windows является важнейшей частью операционной системы. Без него невозможна не только работа системы, но и само ее существование. Не останавливаясь на многочисленных функциях и задачах реестра, отмечу, что его можно использовать в качестве инструмента настройки. С его помощью можно оптимизировать работу как операционной системы, так и многих популярных приложений.

Эти возможности реестра как магнитом притягивают к себе многих пользователей. Начинаются всевозможные эксперименты, связанные с редактированием реестра вручную и с помощью различных сомнительных утилит, которых в Интернете имеется великое

множество. Нередко в результате подобных действий реестр приходит в такое состояние, что система начинает работать нестабильно или просто отказывается загружаться.

Если вам очень хочется поэкспериментировать с реестром, то, по крайней мере, обязательно создайте его резервную копию, причем не только на жестком диске, но и на внешнем носителе информации. Для этого в окне редактора реестра следует выполнить команду главного меню Файл ▸ Экспорт (при этом курсор должен быть установлен в корневую позицию иерархии реестра). При выполнении данной команды на экране появится окно Экспорт файла реестра, в котором по обычным правилам Windows следует указать путь для сохранения. Однако в любом случае без крайней нужды вносить изменения в системный реестр категорически не рекомендуется.

Неаккуратное обращение с реестром часто приводит к необходимости переустановки операционной системы. Однако в последних версиях Windows (начиная с Windows 2000) реализована возможность отката настроек операционной системы к какому-либо предыдущему состоянию. Данная функция называется Восстановление системы.

Чтобы перейти в режим восстановления системы, следует выполнить команду Пуск ▸ Все программы ▸ Стандартные ▸ Служебные ▸ Восстановление системы. С помощью данной функции можно восстановить состояние системы, зафиксированное в определенной точке восстановления на установленную дату (такие точки создаются как вручную, так и автоматически). Подробное описание этого процесса приведено ниже, в соответствующем разделе. Здесь отмечу, что, конечно, восстановление системы позволяет избавиться от многих искусственно созданных проблем, но если операционная система отказывается загружаться, то это средство, разумеется, уже не поможет.

К плачевным результатам может также привести безграмотное редактирование системных и загрузочных файлов (config.sys, boot.ini, pagefile.sys и др.).

В большинстве современных файловых менеджеров (например, Total Commander, Far Manager и др.) имеется режим отображения информации, при использовании которого системные и загрузочные файлы не показываются. Настоятельно рекомендуется включить такой режим, чтобы не было соблазнов редактировать эти файлы (разумеется, если вы дорожите информацией, хранящейся в компьютере).

Что побуждает пользователей редактировать системные и загрузочные файлы? Примерно то же, что и в случае с системным реестром: оптимизация работы системы, настройка параметров загрузки и др. В результате неквалифицированного редактирования файла, например boot.ini, могут возникнуть проблемы с загрузкой операционной системы.

Многие пользователи, купив компьютер и нахватавшись поверхностных знаний о его устройстве, начинают считать себя великими специалистами в этом вопросе. При этом они совершенно не учитывают, что компьютер — это тонкий и деликатный механизм, который не прощает грубого вмешательства. Все его составляющие подобраны таким образом, что представляют собой единую конфигурацию, нарушение которой чревато большими неприятностями. Необходимо помнить и о таком важном факторе, как совместимость: например, оперативная память, успешно работающая на одном компьютере, может отказаться работать на другом, так как она несовместима с установленным на нем оборудованием.

Повреждение жесткого диска

Жесткий диск представляет собой своеобразное хранилище всех данных, находящихся в компьютере. Если при повреждении или выходе из строя любого другого оборудования (например, оперативной памяти или материнской платы) хранящаяся в компьютере информация, как правило, не пропадает, то с жестким диском ситуация иная. Если винчестер поврежден или сбилась его разметка, то вся хранящаяся на нем информация (как операционная система, так и всевозможные файлы и приложения) будет, скорее всего, утеряна.

Тем не менее можно попытаться восстановить хотя бы часть информации. При этом необходимо учесть, что процесс восстановления может быть достаточно трудоемким, а получение положительного результата не гарантировано. В большинстве случаев с поврежденного жесткого диска можно восстановить только небольшие файлы размером до 150 Кбайт.

Подробно рассматривать способы восстановления информации с поврежденного жесткого диска сейчас не будем, поскольку об этом рассказано ниже, в соответствующем подразделе.

Отмечу, что для восстановления данных можно обратиться к специалистам. Однако при этом следует учитывать, что, скорее всего,

полностью восстановить данные все равно не удастся, а финансовые затраты наверняка будут достаточно велики.

Уязвимые места компьютера

Несмотря на то что при грамотном использовании компьютера его надежность намного повышается, в любом случае существуют уязвимые места, которым нужно уделять особое внимание. Некоторые из них находятся в аппаратной части компьютера, остальные (таких большинство) — в программной. Рассмотрим и те, и другие более подробно.

Аппаратная часть компьютера

Какие же компоненты аппаратной части компьютера наиболее подвержены поломкам?

В первую очередь, это блок питания, жесткий диск, материнская плата и монитор. Могут возникать проблемы с оперативной памятью, однако в этом случае чаще всего причина неисправности не в самой оперативной памяти, а в чем-то другом. Например, в результате попадания пыли могут пропадать контакты. В последнем случае пользователь может самостоятельно устранить проблему, если, конечно, знает, где в системном блоке находится оперативная память и как ее нужно снимать и устанавливать. Необходимо снять память и осторожно протереть ее (особенно контактную группу) мягкой сухой материей, после чего вернуть на место.

Если возникают проблемы с аппаратной частью компьютера, то сразу после его включения об этом сигнализирует BIOS. В этой системе предусмотрен набор определенных звуковых сигналов для каждой нестандартной ситуации. Если проблем нет, то любая BIOS выдает один короткий сигнал; остальные сигналы могут различаться в зависимости от модели BIOS: например, один длинный и три коротких звуковых сигнала в AwardBIOS означают наличие проблем с клавиатурой, а в AMIBIOS или в PhoenixBIOS сигнализируют об ошибке оперативной памяти.

Однако необходимо учитывать, что BIOS может и не сообщить о неполадках с «железом». Например, я столкнулся с такой ситуацией: операционная система по непонятным причинам не загружалась, а BIOS выдавала один короткий сигнал, означающий, что с аппаратной частью все в порядке. Попытки переустановить систему

с загрузочного компакт-диска ни к чему не привели — переустановка прекращалась на начальном этапе (компьютер «зависал»). В данном случае помогло только знание уязвимых мест собственного компьютера: пришлось просто достать оперативную память, протереть ее тряпочкой и вновь поставить на место. После этого все проблемы исчезли, а операционная система вновь стала загружаться (ее даже не пришлось переустанавливать). Таким образом, несмотря на общие закономерности, каждый компьютер имеет свои индивидуальные уязвимые места. Если пользователь знает о них, то это избавит его от многих дополнительных проблем.

Как отмечалось, к уязвимым компонентам аппаратной части компьютера можно отнести монитор. Несмотря на то что в настоящее время на отечественном рынке представлен широкий ассортимент высококачественных мониторов, они нередко выходят из строя, не отработав даже гарантийный срок службы. Причина такой ситуации кроется не в качестве мониторов, а в качестве используемых электрических сетей (напомню, что подавляющее большинство электросетей на территории СНГ не имеет заземления). Чтобы сделать вероятность поломки монитора минимальной, рекомендуется обязательно отключать его от сети после окончания работы (некоторые пользователи не выключают монитор сутками, независимо от того, работает он или нет). Следует также избегать автоматического переключения режимов (например, перехода в экономный режим после простоя в течение определенного промежутка времени), так как при отсутствии заземления это повышает риск выхода монитора из строя. Кстати, по этой же причине не рекомендуется слишком часто использовать ждущий и спящий режимы работы компьютера: при этом повышается вероятность выхода из строя какого-либо устройства.

Если блок питания полностью вышел из строя, то компьютер включить не удастся. Однако в большинстве случаев блок питания ломается не моментально. Перед этим пользователь замечает признаки нестабильной работы; например, компьютер может произвольно перезагружаться. При появлении подобных симптомов следует немедленно выяснить, чем они вызваны. Это может быть как неисправность блока питания (в первую очередь нужно проверить, не перегревается ли он), так и проблемы с жестким диском. В последнем случае возможно появление дополнительных симптомов: заметное снижение быстродействия работы компьютера, увеличение

шума, издаваемого жестким диском при работе, и возникновение ошибок при чтении файлов. Если присутствует хотя бы один из этих признаков, то следует немедленно позаботиться о сохранении всех важных данных на внешнем носителе информации — в противном случае велик риск их безвозвратной потери.

Материнская плата — один из важнейших компонентов персонального компьютера. Она координирует и сводит воедино работу других механизмов и компонентов. Если выходит из строя материнская плата, то возможные последствия зависят от характера неисправности. При частичных поломках нередко можно продолжать работу на компьютере — это касается, например, выхода из строя некоторых портов. Если же материнская плата полностью неисправна (например, перегорела в результате перепадов напряжения), то работа на компьютере становится невозможной.

При возникновении подозрений о частичном выходе из строя материнской платы настоятельно рекомендуется выявить и устранить неисправности (вплоть до замены материнской платы). В некоторых случаях частичная поломка материнской платы может привести к выходу из строя другого оборудования, в частности процессора и оперативной памяти.

Программная часть компьютера

Как отмечалось, большинство уязвимых мест компьютера находится в его программной части. Возникновение подобных проблем обусловлено множеством факторов:

- неквалифицированные или ошибочные действия пользователя;
- конфликтные ситуации, возникающие между разными приложениями или приложением и операционной системой;
- нестабильная работа операционной системы;
- программные ошибки, от которых не застраховано ни одно приложение;
- действия вредоносных программ (вирусов, троянских коней) и др.

Какие же программные места компьютера наиболее уязвимы?

Если говорить об операционной системе Windows, то в первую очередь следует обратить внимание на системный реестр. В немалой степени его уязвимость обусловлена тем, что многие пользователи в стремлении оптимизировать работу системы, настроить ее

«под себя» и повысить быстродействие ставят над реестром всевозможные эксперименты. Как уже говорилось, это нередко приводит к прямо противоположному результату.

Кроме этого, в системном реестре зарегистрированы многие установленные на компьютере приложения. Поэтому при удалении программ следует не просто удалить соответствующую папку из каталога Program Files (или другого места, где установлена программа), а воспользоваться специально предназначенной функцией Windows. Для этого следует выполнить команду Пуск ▸ Панель управления ▸ Установка и удаление программ. Однако даже в этом случае не все программы полностью удаляют следы своего пребывания на компьютере. Со временем подобные «хвосты» накапливаются в реестре, что никак не способствует стабильной работе системы (о борьбе с нестабильностью операционной системы рассказано в соответствующем подразделе).

Немалый ущерб системному реестру могут причинить различного рода вирусы. О разновидностях вирусов и о том, как с ними бороться, также рассказано в соответствующем разделе.

Следует отметить, что операционные системы семейства Windows достаточно уязвимы. Это связано в первую очередь не с какими-то их конструктивными недостатками, а с тем, что из-за широкой распространенности они хорошо изучены хакерами, взломщиками и подобными «деятелями». Поэтому корпорация Microsoft периодически выпускает всевозможные «заплатки» для повышения защищенности системы.

Операционные системы UNIX и Linux с точки зрения защищенности выглядят более предпочтительно (в первую очередь потому, что они не так досконально изучены распространителями вредоносных программ). Однако в настоящее время они не получили такого широкого распространения, как системы семейства Windows.

К достаточно уязвимым приложениям можно отнести браузер Internet Explorer и почтовые программы Microsoft Outlook и Outlook Express. Причины их уязвимости те же, что и операционной системы Windows: данные программы широко распространены и хорошо изучены как пользователями, так и распространителями вредоносных программ. В настоящее время становится все более популярным интернет-обозреватель Opera. Он имеет не меньше уязвимых мест, чем Internet Explorer, но ввиду слабой изученности считается более надежным с точки зрения безопасности.

В настоящее время все большее распространение получает кража всевозможных паролей. В результате приложения или ресурсы, для доступа к которым используется пароль, могут неожиданно стать совершенно незащищенными. Разные вредоносные программы, внедренные в компьютер без ведома пользователя (как правило — через Интернет), используют множество способов для кражи пароля. Например, пароль может быть считан с клавиатуры при вводе пользователем, после чего автоматически отослан по адресу, заложенному во внедренной программе. Иногда такая программа выводит на экран ложное диалоговое окно для ввода пароля; пользователь, уверенный в полной защищенности приложения (ресурса), сам вводит пароль, который тут же попадает к злоумышленнику.

Помимо этого, программные ошибки могут возникать по причине того, что разные приложения используют одни и те же библиотеки или ресурсы, что нередко приводит к конфликтам, которые могут закончиться потерей данных. Чем больше приложений и программ установлено на компьютере, тем выше вероятность возникновения различных конфликтных ситуаций. Следует учитывать, что некоторые современные приложения корректно работают только при соблюдении определенной конфигурации оборудования.

2. Вирусы и антивирусы

Наверное, сегодня невозможно встретить пользователя персонального компьютера, который не слышал бы о компьютерных вирусах. Такие вредоносные программы в огромном количестве «представлены» в Интернете. Самое неприятное, что многие распространители вирусов успешно применяют в своей практике передовые достижения IT-индустрии. В результате то, что должно служить во благо пользователям, в конечном итоге может обернуться для них большими проблемами.

Что же включает в себя понятие «компьютерный вирус»? Многие специалисты расходятся во мнениях на этот счет и предлагают разные формулировки. Будем считать, что вирус — это вредоносная программа, проникающая на компьютер без ведома пользователя (хотя, возможно, при невольном его участии) и выполняющая определенные действия деструктивной направленности. Часто вирусы способны к размножению и самораспространению.

Первый компьютерный вирус был написан в начале 80 годов прошлого столетия. Это было не попыткой навредить кому-либо, а сделано просто из интереса. Знал бы автор того вируса, к каким последствиям приведет его развлечение! В настоящее время известно более 150 000 вирусов, и их количество растет с каждым днем.

Каковы же причины возникновения вирусов? Как уже говорилось, на заре «вирусописания» это были просто эксперименты. Постепенно пользователи, умеющие разрабатывать вирусы, стали применять свое умение на практике. Для шутки или розыгрыша использовались относительно безвредные вирусы, не приносящие вреда компьютеру и хранящейся в нем информации. Например, в процессе работы на экране могла внезапно появиться надпись Хочу пива!, убрать которую никак не удавалось. Секрет был прост: нужно было просто ввести слово Пиво.

В конечном итоге вирусы стали создавать с конкретными целями. Например, сотрудник, вынужденный уволиться с работы и считающий себя обиженным, с помощью вируса мог «отомстить» своему бывшему работодателю или коллегам по работе. Кстати, подобные

ситуации возникали и в корпорации Microsoft. Известны случаи, когда ее бывшие сотрудники создавали вирусы, используя знание уязвимых мест операционной системы Windows или офисных приложений.

В настоящее время в мире появилось великое множество «вирусописателей». Одни занимаются созданием и распространением вирусов в качестве хобби, другие просто желают «сделать всем плохо», третьи сводят с кем-то счеты, четвертые имеют вполне конкретные коммерческие цели. Это может быть хищение информации или денежных средств, вывод из строя сетей и веб-ресурсов за солидное вознаграждение (в частности, это является одним из проявлений современной конкурентной борьбы) и т. д.

Все известные вирусы можно классифицировать по нескольким признакам. О видах вирусов вы прочтете в следующем разделе.

Разновидности вирусов

В настоящее время не существует единой классификации вирусов. Одни предлагают использовать в качестве критерия среду обитания вируса, другие — его разрушительные способности, третьи — способ распространения и т. п. Рассмотрим виды вирусов по наиболее характерным признакам.

Известные вирусы можно разделить на следующие группы:

- файловые вирусы;
- сетевые вирусы («черви»);
- загрузочные вирусы;
- макровирусы;
- троянские кони.

Рассмотрим подробнее каждый из перечисленных видов.

Пик распространения файловых вирусов пришелся на конец 80 — начало 90 годов прошлого столетия. Отличительной чертой таких вирусов является то, что они инициируются при запуске зараженной программы. Код вируса скрывается или в исполняемом файле этой программы (файл с расширением EXE или BAT), или в какой-либо динамической библиотеке (DLL), которую использует эта программа. После активизации файловый вирус способен инфицировать другие программы, установленные на компьютере.

Следует, однако, отметить, что время файловых вирусов заканчивается. Исключение составляют только те из них, которые представ-

ляют собой сценарии. Такие вирусы, как правило, входят в состав веб-страниц и написаны с использованием языка сценариев (например, JavaScript).

Основное место «проживания» и функционирования сетевых вирусов («червей») — локальная сеть. Обычно сетевой вирус, попадая в один компьютер, самостоятельно распространяется по остальным компьютерам, входящим в состав сети. Некоторые сетевые вирусы могут использовать своеобразную «приманку», чтобы инициировать свое выполнение. Например, на Рабочем столе зараженного компьютера может внезапно появиться значок с текстом вроде Нажми меня или Срочное сообщение; после щелчка на таком значке вирус активизируется.

Характерной особенностью загрузочных вирусов является то, что они поражают загрузочную область диска (как жесткого, так и гибкого). Такой вирус действует следующим образом. При загрузке компьютера данные из зараженной загрузочной области поступают в память компьютера. После этого инфицируются загрузочные области всех имеющихся жестких дисков, а также доступных дискет. В настоящее время загрузочные вирусы слабо распространены, поскольку основной способ их размножения — через загрузочные дискеты, которые сегодня мало кто использует.

Многие специалисты сходятся во мнении, что большое будущее имеют макровирусы. По структуре они напоминают файловые вирусы, поскольку также существуют в тексте программного кода. Среда обитания макровирусов — макросы, то есть программы, написанные на языке программирования Visual Basic Application. Макросы обычно используются в приложениях Word и Excel с целью расширения их возможностей. Следует отметить, что в последних версиях Windows защита от макровирусов существенно доработана, однако этого все равно недостаточно: создатели макровирусов постоянно совершенствуют свое «мастерство». Пользователь, знакомый с языком программирования Visual Basic Application, может самостоятельно распознать вредоносный код в составе кода программы (особенно если он создал макрос самостоятельно). Однако такой подход целесообразен только тогда, когда макросов используется немного или когда точно известно, в каком из них поселился вирус.

Широкое распространение в настоящее время получили так называемые троянские кони. Их отличительной особенностью являет-

ся то, что они, как правило, не причиняют ущерб компьютеру или хранящейся в нем информации. Основное функциональное назначение таких программ — предоставить свободный доступ к данному компьютеру через Интернет. При этом удаленный пользователь может делать с зараженным компьютером все что угодно: удалять и записывать информацию, редактировать параметры настройки, запускать программы и т. д.

Цели могут преследоваться совершенно разные: кража конфиденциальной информации, взлом паролей, рассылка спама и др. Причем если с зараженного компьютера, например, рассылается спам, то всю ответственность за это будет нести ничего не подозревающий владелец этого компьютера, а не удаленный пользователь, реально управляющий данным процессом. Таким образом, основное коварство троянских коней заключается в том, что пользователь зараженного компьютера не подозревает о том, что его компьютер используется посторонними лицами (причем нередко — в противозаконных целях).

Для эффективной защиты от троянских коней недостаточно антивирусной программы. Кроме нее необходимо также использовать брандмауэр. Подробнее о таких защитных программах рассказано в разд. 4.

Помимо перечисленных разновидностей вирусов, в Интернете существуют вирусы, которые можно отнести одновременно к нескольким группам. Такие вирусы иногда называют смешанными.

Лучшие антивирусные программы

Как уже отмечалось, в настоящее время в Интернете существует великое множество разнообразных вирусов. Поэтому на любом современном компьютере должна быть установлена антивирусная программа. Перечислю наиболее популярные из них, а в качестве примера использования антивируса рассмотрим порядок работы с программой Антивирус Касперского Personal.

В настоящее время на отечественном компьютерном рынке представлено множество самых разнообразных антивирусных программ. Некоторые из них распространяются бесплатно, некоторые — на платной основе. Следует отметить, что эффективность платных антивирусных программ существенно выше, чем бесплатных. Поэтому для надежной защиты компьютера (особенно при частом исполь-

зовании Интернета, а также при работе в локальной сети) рекомендуется установить платную антивирусную программу.

Признанными лидерами антивирусных программ в настоящее время являются программы Антивирус Касперского Personal, Dr.Web и Norton Antivirus. Все они являются платными. Остановимся подробнее на каждой из них.

Антивирус Касперского Personal

Программа Антивирус Касперского Personal разрабатывается и поддерживается известной лабораторией Касперского. Данную антивирусную программу подробно рассмотрим в подразд. «Работа с программой Антивирус Касперского Personal».

Dr.Web

Программа Dr.Web является одной из первых отечественных антивирусных программ и в настоящее время относится к наиболее популярным. Немаловажным достоинством программы является ее относительно невысокая стоимость по сравнению с другими разработками аналогичного уровня.

При инсталляции Dr.Web пользователю предлагается выбрать требуемый вариант установки: Типичная, Минимальная и Выборочная. В большинстве случаев рекомендуется выбрать вариант Типичная, заданный по умолчанию. Следует учитывать, что после инсталляции программы необходимо перезагрузить компьютер (вы увидите соответствующее информационное сообщение).

Программа Dr.Web предусматривает использование двух языков интерфейса: русского и английского. Требуемый язык выбирают при инсталляции программы, однако в дальнейшем при необходимости его можно изменить.

В состав программы входит несколько самостоятельных модулей, которые, как правило, работают независимо друг от друга, хотя используют одну и ту же антивирусную базу. На первых порах это может вызывать определенные затруднения, но уже через некоторое время неудобства исчезнут.

Модуль Dr.Web для Windows представляет собой инструмент для сканирования компьютера или выбранных объектов на предмет заражения вирусами. После установки программы вы сможете вызвать сканер с помощью соответствующей команды контекстного меню

значка объекта в окне Проводника. При выполнении данной команды выбранный объект будет проверен на наличие вирусов.

Параметры сканирования устанавливают в настройках программы. В частности, там указывают объекты, которые нужно проверить, определяют порядок действий в случае обнаружения вируса (переименовать зараженный объект, удалить его, вылечить или поместить в указанную папку), устанавливают количество ресурсов компьютера, выделяемых на сканирование, и др.

Модуль Spider Mail представляет собой почтовый сканер и предназначен для проверки почтовых сообщений на предмет заражения их вирусами. Эту возможность настраивают отдельно — для нее предусмотрены специальные параметры.

Следует отметить, что почтовый сканер Spider Mail отличается высокой надежностью.

В состав программы также входит файловый сканер Spider Guard. Этот модуль предназначен для проверки файлов на наличие вирусов в тот момент, когда с ними выполняют определенное действие (запускают, записывают на диск и др.). Данная функция также отличается высокой надежностью — многие специалисты считают именно ее самым сильным местом программы.

В процессе работы программы Dr.Web в области уведомлений Панели задач отображаются значки используемых в данный момент модулей.

Norton Antivirus

Программа Norton Antivirus — также очень популярная в настоящее время антивирусная программа. Ее разработчиком является всемирно известная фирма Symantec. По сравнению с программами Антивирус Касперского Personal и Dr.Web этот антивирус обладает для отечественного пользователя одним существенным недостатком: он не поддерживает русский язык. Тем не менее некоторые пытаются применить к нему различного рода русификаторы, и иногда это приносит определенный успех.

Разработчиками предусмотрены разные конфигурации программы: для домашнего и офисного применения. Средняя стоимость «домашней» версии составляет около $50.

Процесс инсталляции этого антивируса несложен и доступен даже начинающему пользователю. Однако необходимо учитывать, что после завершения установки требуется перезагрузить компьютер.

Norton Antivirus имеет приятный и эргономичный интерфейс. По мнению многих пользователей, он намного более современный, чем интерфейсы рассмотренных выше программ Dr.Web и Антивирус Касперского Personal.

К несомненным достоинствам программы следует отнести возможность автоматического обновления антивирусных баз без участия пользователя. Разумеется, необходимое условие — наличие действующего подключения к Интернету.

В данной программе реализована очень мощная функция проверки электронной почты. При этом поддерживается работа с наиболее популярными почтовыми программами: Outlook Express, Microsoft Outlook, The Bat! и др. Использование Norton Antivirus практически полностью исключает возможность приема и отправки электронных сообщений, зараженных вирусами.

Для запуска процесса сканирования компьютера (или выбранных объектов) предназначена кнопка Scan Now (Сканировать сейчас), которая расположена в правом нижнем углу окна программы.

К недостаткам рассматриваемого антивируса можно отнести то, что процесс сканирования компьютера (или указанных объектов) требует слишком много ресурсов компьютера, в результате чего заметно замедляется быстродействие или работа вообще становится невозможной. Однако высокое качество сканирования с лихвой компенсирует этот недостаток.

Обнаруженные в процессе сканирования вирусы и зараженные файлы помещаются в специальную папку. После этого пользователь может досконально с ними разобраться и, в зависимости от полученного результата, удалить файлы или вернуть их на прежнее место.

Прочие антивирусные программы

В данном подразделе кратко рассмотрим несколько антивирусных программ, которые хоть и не настолько распространены, как описанные выше, но, на мой взгляд, достойны упоминания в книге.

Stop! Антивирусная программа Stop! также является платной. Бесплатную демонстрационную версию с ограниченными возможностями можно использовать только в течение 30 дней после установки; вы можете скачать ее по адресу http://www.proantivirus.com/ru/download. Несомненным достоинством программы является ее мультиязычность: Stop! поддерживает русский, английский, немецкий, болгарский, украинский и эстонский языки.

В состав стандартного пакета программы включено несколько модулей: Монитор, Обновление, Сканер и E-Mail Guardian.

Модуль Сканер предназначен для сканирования компьютера или выбранных объектов на предмет заражения вирусами. Перед запуском процесса сканирования рекомендуется просмотреть и при необходимости отредактировать параметры сканирования. В частности, в режиме настройки можно указать объекты для проверки (например, файлы, папки, архивы) и определить порядок действий при обнаружении вируса (лечить, удалить и т. д.). В любой момент сканирования можно просмотреть динамически изменяющуюся информацию о количестве проверенных объектов, обнаруженных вирусов и др.

С помощью модуля Монитор антивирусная программа наблюдает за состоянием компьютера и находящихся в нем данных. Предусмотрена отдельная настройка режима мониторинга. Следует учитывать, что при включении данного режима быстродействие работы компьютера может снизиться.

Поскольку большинство пользователей получают основную часть вирусов через электронные почтовые сообщения, в программе Stop! реализована возможность проверки электронной почты. Для этого предназначен специальный модуль — E-Mail Guardian, который проверяет входящие почтовые сообщения. Данный модуль работает с большинством популярных почтовых программ — в частности, Microsoft Outlook, Outlook Express, The Bat! и др. Следует отметить, что в отличие, например, от Norton Antivirus программа Stop! не проверяет исходящие почтовые сообщения.

Модуль Обновление используется для автоматического обновления антивирусных баз через Интернет (разумеется, для этого необходимо наличие действующего подключения к Интернету). Кроме этого, обновлять базы можно вручную: для этого нужно скачать их с сайта разработчика программы.

Наряду с большим количеством преимуществ, программа Stop! имеет два существенных недостатка. Первым из них является сравнительно небольшое количество вирусов, содержащихся в антивирусной базе этой программы (примерно в полтора раза меньше, чем у Dr.Web и Norton Antivirus, и в два раза — чем у Антивирус Касперского Personal). Отмечу, что самое большое количество вирусов известно антивирусной базе программы Антивирус Касперского Personal. Второй недостаток программы Stop! — она очень слабо распознает

макровирусы, которые в настоящее время широко распространены и доставляют пользователям массу проблем.

Panda Antivirus. Разработчиком антивирусной программы Panda Antivirus является испанская фирма Panda Software. Стоимость этого антивируса составляет примерно €35.

В состав программы входят модули сканирования и мониторинга (эти функции в Panda Antivirus объединены), почтового сканирования (для проверки электронной корреспонденции) и автоматического обновления антивирусных баз.

К характерным особенностям (преимуществам) программы относится то, что после установки ее практически не нужно настраивать. Конечно, при необходимости пользователь может настроить любые параметры в соответствии со своими потребностями. Однако значения, предлагаемые по умолчанию, подобраны настолько оптимально, что в большинстве случаев программу можно использовать непосредственно после инсталляции. Одним из приоритетных направлений, заложенных в программе, являются простота и удобство работы с ней даже для неопытных и начинающих пользователей.

Отдельно следует отметить возможность программы восстанавливать поврежденную вирусом систему. Иначе говоря, после обнаружения вируса и его обезвреживания (удаления или лечения) программа ликвидирует все связанные с ним изменения в системных файлах, реестре и настройках системы, после чего возвращает операционную систему в то состояние, в котором она была до появления вируса.

Virus Scan. Разработчиком программы Virus Scan является американская корпорация McAfee. В данной программе, как и во многих других, реализовано два основных направления: для домашних компьютеров и офисного применения.

Стоимость программы составляет около $50. Однако вы можете скачать с сайта разработчика бесплатную демонстрационную версию, которая действительна в течение 15 дней с момента инсталляции.

Программа обладает достаточно удобным, современным и эргономичным пользовательским интерфейсом. Существенный, с точки зрения отечественных пользователей, недостаток — поддержка только английского языка.

Антивирусную программу Virus Scan можно приобрести как отдельно, так и в комплексе с другими программами этого же разработчика,

предназначенными для защиты компьютера и информации, — в частности, с антиспамовым фильтром и брандмауэром. Всеми инструментами программы управляют из одного окна — McAfee Security Center. Переключаться между режимами можно с помощью соответствующих вкладок.

Работа с программой Антивирус Касперского Personal

Антивирус Касперского Personal является одной из наиболее популярных антивирусных программ. К ее достоинствам можно отнести простой и интуитивно понятный пользовательский интерфейс, возможность гибкой настройки параметров сканирования, а также наличие богатой антивирусной базы (на момент написания книги в антивирусной базе программы насчитывалось более 155 000 вирусов, и этот список пополняется ежечасно).

В этой книге мы рассмотрим порядок работы с программой Антивирус Касперского Personal на примере версии 5.0.390 — последней на момент написания книги.

Характерным отличием данной версии программы от предыдущих является то, что теперь Антивирус Касперского Personal представляет собой цельный программный продукт, управляемый из одного интерфейса. Предыдущие версии антивируса состояли из набора приложений (Scanner, Monitor и др.), каждое из которых специализировалось на определенном виде защиты, поэтому данная доработка существенно упростила порядок использования программы.

Рабочее окно программы Антивирус Касперского Personal содержит три вкладки: Защита, Настройка и Поддержка. Рассмотрим порядок работы с каждой вкладкой.

Защита

Вкладка Защита (рис. 2.1) по умолчанию открывается при запуске программы.

В правой части данной вкладки приводится справочная информация о текущем состоянии антивирусной защиты компьютера. Например, на рис. 2.1 видно, что программа сообщает о необходимости выполнить полную проверку компьютера на предмет заражения вирусами и ожидает соединения с Интернетом для обновления антивирусных баз. Кроме этого, сообщается о том, что в текущем се-

ансе работы была обнаружена одна сетевая атака, а также об установленном уровне антивирусной защиты.

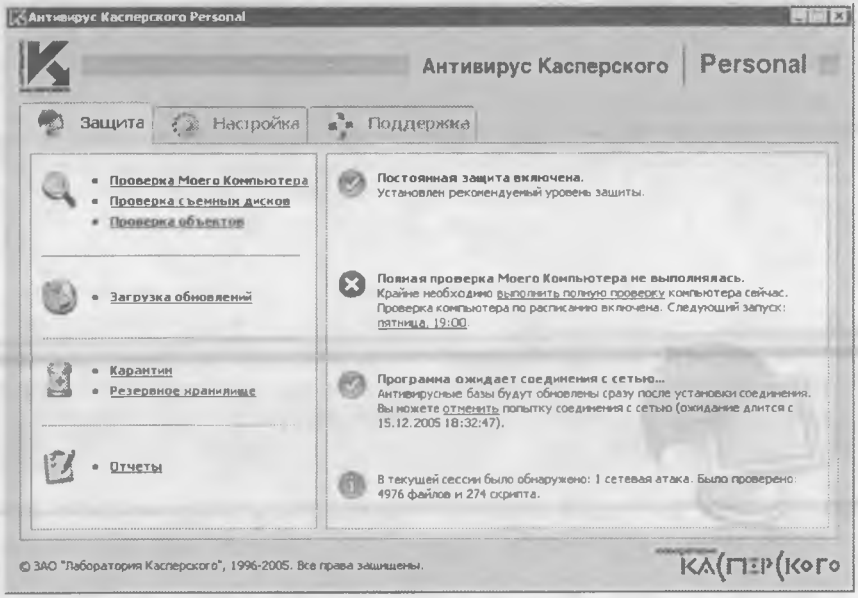

Рис. 2.1. Вкладка Защита

В левой части вкладки находятся ссылки, с помощью которых можно перейти в соответствующие режимы работы. Рассмотрим эти ссылки.

Чтобы начать полное сканирование компьютера на наличие вирусов и иных вредоносных программ, щелкните на ссылке Проверка Моего Компьютера. При этом на экране появится окно (рис. 2.2), в котором можно наблюдать за процессом сканирования (здесь отображается количество проверенных и удаленных объектов, обнаруженных и вылеченных вирусов и др.).

Чтобы временно остановить сканирование, следует нажать в данном окне кнопку Пауза (после нажатия эта кнопка изменит имя на Продолжить и будет предназначена для возобновления процесса сканирования). С помощью кнопки Стоп можно досрочно прекратить сканирование (без видимых причин нажимать эту кнопку не рекомендуется).

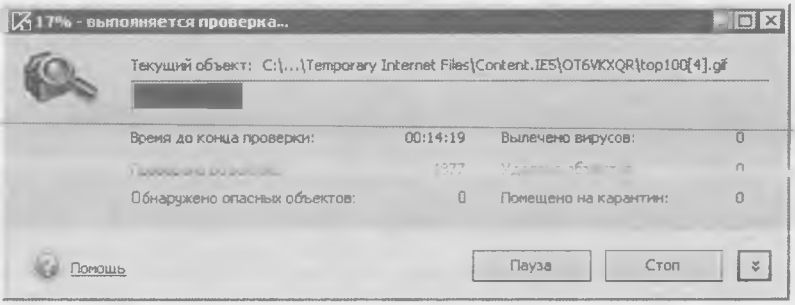

Рис. 2.2. Полное сканирование компьютера

Для сканирования только съемных дисков (дискет, компакт-дисков, DVD и др.) следует воспользоваться ссылкой Проверка съемных дисков.

При необходимости можно выполнить выборочное сканирование хранящихся на компьютере объектов. Для перехода в соответствующий режим предназначена ссылка Проверка объектов. После щелчка на этой ссылке на экране появится окно Выбор объектов для проверки (рис. 2.3).

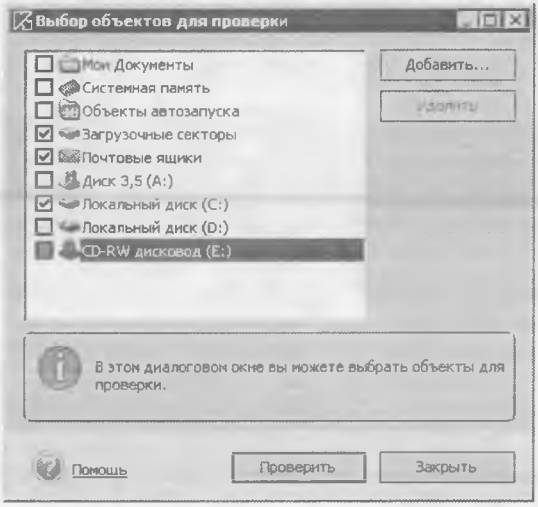

Рис. 2.3. Выбор объектов для сканирования

В данном окне установкой соответствующих флажков выбирают объекты, которые нужно проверить. При необходимости можно

дополнить предложенный список, для чего предназначена кнопка Добавить. При нажатии данной кнопки на экране появится окно, в котором следует указать путь к требуемому объекту и нажать кнопку Выбрать. Добавленный таким образом объект впоследствии можно удалить из списка — для этого нужно установить на него курсор и нажать кнопку Удалить. Следует отметить, что из списка можно удалять только добавленные пользователем объекты. На рис. 2.3 показан список, предложенный программой по умолчанию. Из такого списка удалить ничего нельзя (кнопка Удалить доступна только при выборе объекта, добавленного пользователем). Выбрав объекты для проверки, следует нажать кнопку Проверить, чтобы запустить процесс сканирования.

Ссылка Загрузка обновлений предназначена для обновления антивирусных баз. Следует отметить, что возможности программы предусматривают автоматическое обновление антивирусных баз в соответствии с установленным расписанием. О настройке автоматического обновления рассказано ниже, в подразд. «Вкладка Настройка». С помощью ссылки Загрузка обновлений можно запустить внеочередное обновление антивирусных баз. Базы могут обновляться как из расположенной на компьютере локальной папки, так и через Интернет с сайта программы (в последнем случае необходимо наличие действующего подключения к Интернету). Способ обновления задает пользователь.

С помощью ссылки Карантин можно перейти в режим работы с подозрительными объектами, помещенными на карантин пользователем или программой Антивирус Касперского Personal в процессе проверки. При щелчке на этой ссылке на экране появляется окно, изображенное на рис. 2.4.

Данное окно содержит список объектов, помещенных на карантин. Для каждой позиции списка в соответствующих столбцах указывают имя объекта, его статус (помещен пользователем, не заражен и т. д.), дату помещения на карантин и полный путь к объекту. Объекты, находящиеся на карантине, как бы «блокируются» («замораживаются») и поэтому становятся безопасными.

Как отмечалось, подозрительные объекты могут помещаться на карантин автоматически, в процессе сканирования, или вручную, пользователем. Для ручного добавления объекта на карантин в окне Карантин (см. рис. 2.4) следует нажать кнопку Добавить, после чего в появившемся окне по обычным правилам Windows указать путь

к требуемому объекту. Для восстановления объекта выделите его в списке и нажмите кнопку Восстановить. При этом объект появится на прежнем месте, полностью способный нормально функционировать.

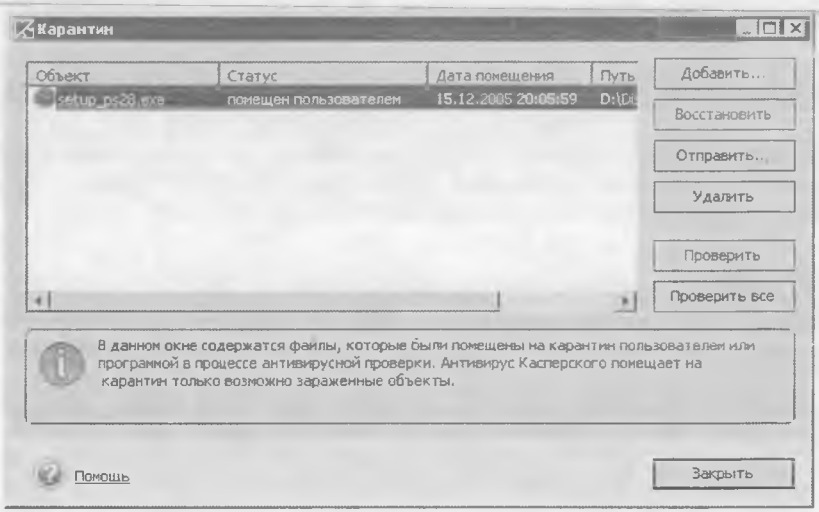

Рис. 2.4. Карантин

Кнопка Отправить предназначена для отправки выбранного объекта на исследование в лабораторию Касперского, для чего необходимо наличие действующего подключения к Интернету. Перед отправкой следует проверить подозрительный объект с использованием самых свежих антивирусных баз (в противном случае отправка будет невозможна). После проверки статус объекта изменится: например, если объект имел статус помещен пользователем, а проверка показала, что он не заражен вирусом, то после проверки этот объект примет статус не заражен.

Для удаления объекта из списка следует установить на него курсор и нажать кнопку Удалить.

С помощью кнопки Проверить можно проверить выбранный в списке объект на предмет заражения вирусами. Кнопка Проверить все предназначена для проверки всех объектов, находящихся на карантине.

При удалении зараженных или подозрительных объектов программа Антивирус Касперского Personal создает их резервные копии. Впоследствии удаленные объекты можно восстановить из этих ко-

пий. Однако учтите, что восстанавливать удаленные объекты из резервных копий следует только в случае крайней необходимости, поскольку это может привести к заражению компьютера.

Для перехода в режим работы с резервными копиями предназначена ссылка Резервное хранилище. При щелчке на этой ссылке на экране появится окно Резервное хранилище, содержащее список созданных резервных копий. Для каждой позиции списка в соответствующих столбцах отображаются имя, статус (например, заражен), дата помещения в хранилище и полный путь к объекту. Для восстановления объекта на прежнем месте нужно выделить его в списке и нажать кнопку Восстановить. Для удаления объектов предназначена кнопка Удалить.

С помощью ссылки Отчеты можно перейти в режим работы с журналом отчетов. После щелчка на этой ссылке откроется окно со списком имеющихся отчетов (например, отчет о проверке почты, отчет о постоянной защите от сетевых атак, отчет о полной проверке компьютера и т. д.). Для просмотра требуемого отчета следует выделить его в списке и нажать кнопку Подробно.

Вкладка Настройка

Содержимое вкладки Настройка (рис. 2.5) предназначено для настройки параметров работы программы.

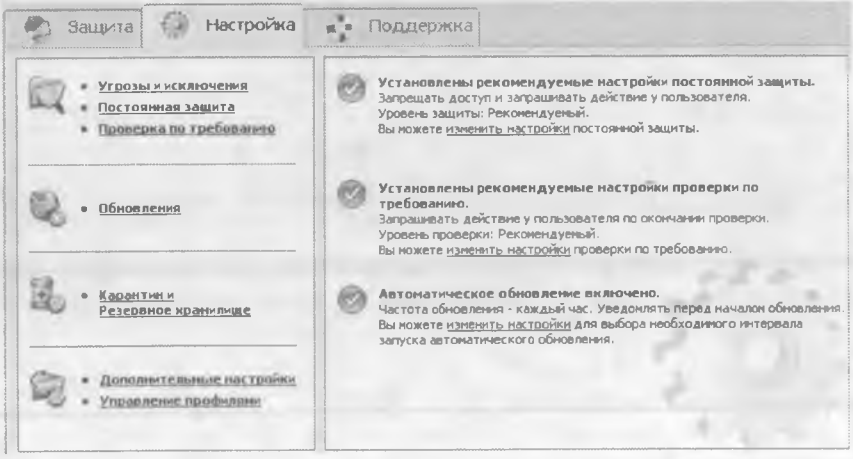

Рис. 2.5. Вкладка Настройка

В правой части вкладки отображается краткая информация о текущем состоянии настроек, в левой части — ссылки, с помощью которых можно перейти в различные режимы настройки программы.

В программе Антивирус Касперского Personal реализована возможность создания и ведения списка исключений — объектов, которые будут игнорироваться при сканировании компьютера. Для перехода в режим работы с этим списком предназначена ссылка Угрозы и исключения. После щелчка на этой ссылке откроется окно, изображенное на рис. 2.6.

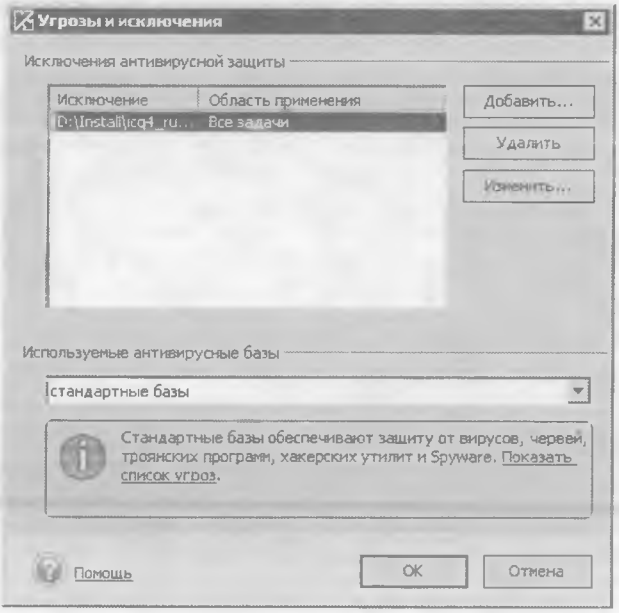

Рис. 2.6. Список исключений

Для добавления в список исключений новой позиции следует нажать кнопку Добавить. В результате откроется окно, в котором в поле Объект следует выбрать исключаемый объект, после чего нажать кнопку ОК. Для удаления объекта из списка исключений необходимо выделить его и нажать кнопку Удалить.

С помощью ссылок Постоянная защита и Проверка по требованию можно перейти соответственно в режим настройки постоянной защиты (постоянного мониторинга) компьютера и проверки компью-

тера, инициированной пользователем. При щелчке на любой из этих ссылок на экране появится окно настройки параметров, в котором с помощью ползунка следует установить требуемый режим проверки (по умолчанию — Рекомендуемый). В этом окне также нужно определить действие программы при обнаружении вируса или подозрительного объекта: удалить объект, спросить о дальнейших действиях у пользователя и др. Кроме этого, вы можете настроить дополнительные параметры. В окне Настройка постоянной защиты для перехода в соответствующий режим следует воспользоваться ссылкой Настройка параметров защиты, а в окне Настройка проверки по требованию — ссылками Настройка проверки по расписанию и Настройка параметров проверки.

Ссылка Обновления предназначена для перехода в режим настройки обновлений антивирусных баз. При щелчке на этой ссылке на экране появится окно, представленное на рис. 2.7.

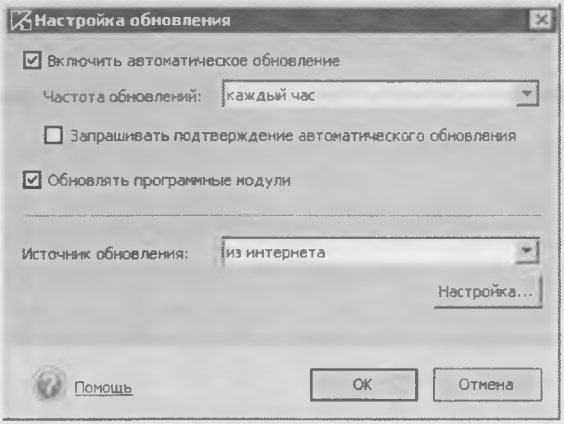

Рис. 2.7. Настройка обновлений антивирусных баз

В программе Антивирус Касперского Personal реализована возможность автоматического обновления антивирусных баз в соответствии с установленным расписанием. Для этого в окне Настройка обновления (см. рис. 2.7) необходимо установить флажок Включить автоматическое обновление, после чего из раскрывающегося списка Частота обновлений выбрать требуемый режим обновления баз: каждый час, каждые три часа, раз в сутки, раз в неделю и др. Если автоматическое обновление отключено, то запустить обновление антивирусных баз

можно щелчком на ссылке Загрузка обновлений, которая расположена на вкладке Защита. С помощью этой ссылки можно выполнять внеочередное обновление антивирусных баз даже при включенном автоматическом обновлении.

В поле Источник обновления выбирают место, откуда будут загружаться обновленные антивирусные базы: из интернета (в данном случае базы будут скачаны с сайта программы при наличии действующего подключения к Интернету) или из локального каталога (из расположенной на компьютере локальной папки).

С помощью ссылки Карантин и Резервное хранилище можно перейти в режим настройки работы с карантином и резервным хранилищем. После щелчка на данной ссылке на экране появится окно, в котором с помощью установки соответствующих флажков можно определить предельный размер карантина и резервного хранилища (в мегабайтах), а также установить количество дней, по истечении которого объекты, помещенные на карантин и в резервное хранилище, будут автоматически удаляться. Кроме этого, в данном окне можно включить режим автоматической проверки объектов, находящихся на карантине, после каждого обновления антивирусных баз.

Для перехода в режим настройки некоторых дополнительных параметров работы программы предназначена ссылка Дополнительные настройки. В открывшемся после щелчка на данной ссылке окне с помощью соответствующих флажков можно включить звуковое оформление работы программы, режим автозагрузки, задать пароль для защиты программы и др.

Ссылка Управление профилями предназначена для сохранения настроек работы антивируса в отдельном конфигурационном файле для последующего использования. При щелчке на данной ссылке на экране появится окно, в котором можно сохранить и восстановить настройки. С помощью расположенной в данном окне кнопки Восстановить профиль восстанавливают настройки работы программы, используемые по умолчанию.

Поддержка

Вкладка Поддержка (рис. 2.8) содержит некоторые сервисные функции программы.

В правой части вкладки Поддержка отображается информация о технической поддержке, используемой версии программы Анти-

вирус Касперского Personal, количестве записей в антивирусных базах и др.

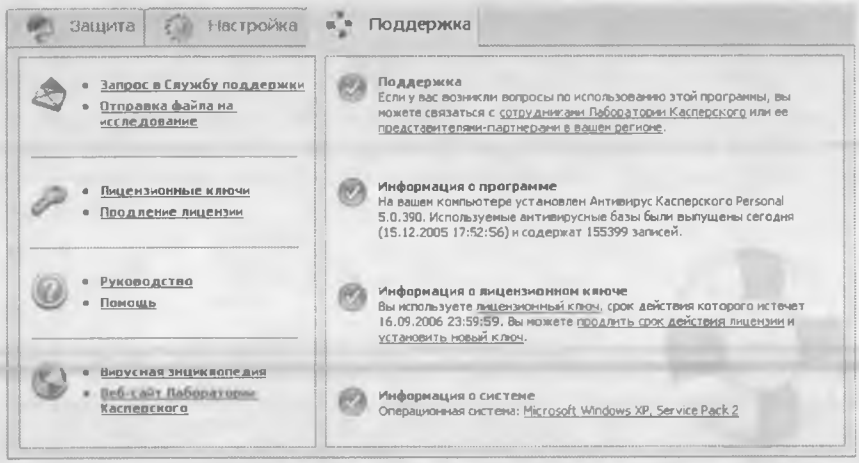

Рис. 2.8. Вкладка Поддержка

Если в процессе эксплуатации программы возникли какие-либо затруднения или проблемы, то можно проконсультироваться со службой технической поддержки. Для немедленной отправки соответствующего запроса предназначена ссылка Запрос в службу техподдержки (учтите, что при этом должно присутствовать действующее подключение к Интернету).

С помощью ссылки Отправка файла на исследование можно отправить в лабораторию Касперского подозрительный файл для проведения дополнительных исследований. После щелчка на данной ссылке на экране появится окно, в котором следует указать путь к подозрительному файлу. Перед отправкой программа автоматически проверит выбранный файл на наличие в нем вредоносного кода и при отсутствии такового выдаст соответствующее предупреждение.

Ссылка Лицензионные ключи предназначена для добавления, обновления или удаления используемых лицензионных ключей. Необходимые действия выполняют в окне Управление лицензионными ключами, которое появляется на экране после щелчка на данной ссылке.

Ссылки Руководство и Помощь предназначены для вызова справочной информации.

Как восстановить работоспособность зараженного компьютера

Несмотря на многообразие представленных на отечественном рынке антивирусных программ и достаточно высокую степень их надежности, ни одна программа не гарантирует стопроцентную защиту компьютера или его содержимого от заражения вирусом. Поэтому в данном разделе рассмотрим, как можно восстановить работу инфицированного компьютера.

Если выяснилось, что компьютер заражен вирусом, то самое главное — не паникуйте и не предпринимайте никаких необдуманных действий и «резких движений»: не следует удалять файлы, перезагружать компьютер и т. п. Необходимо помнить, что в большинстве случаев из подобной ситуации можно выйти без особых потерь, но только тогда, когда все действия четко продуманы. В любом случае заражение вирусом — это не самое страшное, что может случиться с компьютером.

Порядок действий, которые необходимо выполнить для восстановления работоспособности зараженного компьютера, зависит в основном от степени заражения. Одна из самых неприятных ситуаций — когда отказывается загружаться компьютер или операционная система.

Причиной того что компьютер не загружается, может быть повреждение вирусом BIOS. В данном случае начинающим пользователям лучше не предпринимать никаких действий, а обратиться за помощью к специалистам. Отмечу лишь, что, вероятнее всего, придется перезаписывать микросхему BIOS, а эта процедура требует определенного опыта и знаний.

Вирус может не нанести серьезных повреждений BIOS, а только изменить некоторые настройки. Если в результате этого возникнут проблемы с загрузкой компьютера, то наиболее приемлемый выход из данной ситуации — восстановить настройки BIOS, используемые по умолчанию. Для этого нужно войти в BIOS (сразу после включения компьютера необходимо нажать и удерживать клавишу Delete) и найти соответствующую функцию. Название этой функции зависит от версии BIOS, но в любом случае ее найти несложно (она может выглядеть, например, как Fail-Safe Defaults или Load BIOS Defaults).

Однако может возникнуть ситуация, когда компьютер загружается нормально, а операционная система — нет. Иначе говоря, пробле-

мы начинаются после выбора в загрузочном меню требуемой операционной системы. В данном случае можно попробовать загрузить систему в дополнительном режиме. Для выбора нестандартного режима нажмите клавишу F8, находясь в загрузочном меню. При этом на экране появится меню выбора режима загрузки.

В первую очередь рекомендуется выбрать режим Загрузка последней удачной конфигурации. Его смысл заключается в том, что при загрузке операционной системы будут использованы параметры и настройки, которые применялись при ее последнем удачном запуске.

Если в данном режиме загрузиться не удалось, следует выбрать Режим отладки или Безопасный режим. Эти режимы позволяют загрузить операционную систему с некоторым ограничением ее функциональности.

Если операционная система не загружается ни в одном режиме, то, скорее всего, придется искать неисправность в аппаратной части компьютера или переустанавливать систему.

Если удалось загрузить систему в нестандартном режиме, то, в зависимости от степени заражения, рекомендуется выполнить следующие действия.

- Проверить компьютер антивирусной программой (перед этим следует обязательно обновить антивирусные базы).
- Восстановить Windows (для систем версии Windows 2000 и выше). Эта возможность предназначена для отката операционной системы в одно из предыдущих состояний (подробнее об этом читайте в разд. 7). В некоторых случаях восстановление системы позволяет ликвидировать последствия действий вредоносных программ.
- Предпринять все меры для сохранения имеющейся в компьютере информации (особенно если сканирование антивирусом не принесло результатов). Лучше скопировать наиболее важные данные на внешний носитель информации или на сетевой диск — ведь неизвестно, как поведет себя операционная система при следующей загрузке.

В большинстве случаев для решения проблемы заражения вирусами достаточно сканировать компьютер антивирусной программой (конечно, если это хорошая платная программа). Кроме того, некоторые антивирусы имеют средства для отката системы или файлов к «довирусному» состоянию. Однако стоит отметить, что

на должном уровне данная возможность не реализована даже в широкоизвестных антивирусных программах.

При использовании операционной системы Windows XP рекомендуется сохранить на внешнем носителе папку system32/config. Если вирус внес какие-либо изменения в системный реестр или настройки системы, то сохраненную на внешнем носителе папку можно скопировать на прежнее место, заменив при этом ее содержимое. Так можно ликвидировать некоторые последствия действий вируса.

Если операционная система категорически не желает загружаться ни в одном режиме и очевидно, что без ее переустановки (а возможно, и без форматирования жесткого диска) не обойтись, то нужно постараться сохранить имеющиеся в компьютере данные. В таком случае следует загрузиться в режиме MS-DOS с загрузочного компакт-диска (или дискеты) и попытаться перенести данные на внешние носители информации (дискету, компакт-диск, сетевой диск и др.).

Профилактика, или Как уберечься от вирусов

Как отмечалось, стопроцентной защиты от вирусов сегодня не существует. Тем не менее соблюдение следующих правил может многократно снизить риск заражения. Эти правила просты и известны многим пользователям, однако соблюдают их, к сожалению, не все.

- По возможности избегайте компьютеров «общего пользования», установленных в студенческих аудиториях, на почтах и т. п. За день таким компьютером пользуется множество человек, и любой может занести вирус со своей дискеты или компакт-диска. Поэтому записывать информацию с такого компьютера на свою дискету — примерно то же самое, что в разгар эпидемии гриппа посещать многолюдные места.
- При получении из Интернета или локальной сети файлов приложений пакета Microsoft Office (например, Word или Excel) в первую очередь проверьте их надежной антивирусной программой и только потом открывайте. Такие файлы могут содержать макровирусы.
- То же самое относится и к другим скачиваемым из Интернета файлам: дистрибутивам или исполняемым файлам приложений, самораспаковывающимся архивам и др. Перед выполне-

нием их необходимо проверить антивирусной программой (не забыв предварительно обновить антивирусные базы).

- Если используемая антивирусная программа обладает возможностью постоянного мониторинга, то при работе в Интернете данный режим обязательно должен быть включен. Это поможет своевременно обнаружить зараженные файлы, пытающиеся проникнуть в компьютер.
- Время от времени нужно полностью сканировать компьютер на наличие вирусов с помощью хорошей антивирусной программы. Периодичность сканирования зависит от загрузки компьютера, а также от того, работает ли пользователь с Интернетом.
- При работе с внешними носителями информации (например, дискетами или компакт-дисками) обязательно проверяйте их антивирусной программой на наличие вирусов. Особенно это касается работы с чужими или новыми компакт-дисками или дискетами.
- Ни в коем случае не запускайте внезапно появившиеся на Рабочем столе значки. Многие вирусы (особенно сетевые «черви») специально помещают на Рабочий стол заманчивый значок. При щелчке на таком значке вирус активизируется и начинает распространяться по сети.
- Если вы работаете с файлами, расположенными в Интернете, не запускайте их сразу. Сохраните нужный файл на свой компьютер, проверьте его антивирусной программой и только после этого откройте.
- После окончания работы в Интернете обязательно отключите шнур, соединяющий компьютер с телефонной линией. Если этого не сделать, то злоумышленник может легко получить доступ даже к выключенному компьютеру.

3. Другие вредоносные программы и защита от них

В настоящее время жизнь пользователям портят не только разнообразные компьютерные вирусы. Кроме них, в Интернете (и не только в нем) существует множество различных вредоносных программ. В этой книге рассмотрим наиболее распространенные виды таких программ: шпионские модули Spyware и рекламные модули Adware.

Однако в первую очередь перечислю меры предосторожности, соблюдение которых хоть и не исключает, но сводит к минимуму вероятность проникновения в компьютер различных вредоносных программ.

Как обезопасить компьютер от вредоносных программ

Несмотря на то что производители губительного программного обеспечения постоянно совершенствуют методы проникновения в чужие компьютеры, соблюдение следующих несложных мер предосторожности избавит пользователя от многих ненужных проблем.

- При скачивании из Интернета файлов и приложений рекомендуется использовать специально предназначенные для этого программы, в которых предусмотрена возможность просмотра и анализа скачиваемых файлов и архивов (например, Download Master).
- Иногда при щелчке на ссылке для скачивания файла или программы на экране автоматически появляется приглашение перейти по другой ссылке и скачать другую (более дешевую, более современную, более полезную и т. п.) программу. От подобных предложений следует отказываться. В противном случае существует риск получить на свой компьютер целый «набор» вредоносных модулей.
- Существуют приложения, которые при установке добавляют в интерфейс почтовой программы или браузера собственные

элементы управления (кнопки, панели инструментов, пункты меню и т. д.). Такие программы вполне могут включать в себя шпионские или рекламные модули. Разумеется, это не относится ко всем подобным программам, но определенная осторожность при их использовании не помешает. В частности, после установки настоятельно рекомендуется проверить их программой типа Antispyware или Antiadware.

- По возможности не скачивайте из Интернета и не устанавливайте на свой компьютер программы и утилиты неизвестных разработчиков.
- Если вам пришлось установить на компьютер подозрительное приложение, обязательно проверьте его специальной программой типа Antispyware или Antiadware на наличие шпионских и рекламных модулей.

Шпионские модули Spyware и борьба с ними

Основное отличие шпионских модулей Spyware от компьютерных вирусов заключается в том, что они, как правило, не наносят вреда программному обеспечению и данным, хранящимся в компьютере (если не считать занимаемых ими ресурсов оперативной памяти и места на жестком диске). Задача шпионских модулей — собирать некоторую информацию о пользователе (адреса электронной почты, содержимое жесткого диска, список посещаемых страниц в Интернете, информацию личного характера) и отправлять ее по определенному адресу. При этом пользователь даже не подозревает, что за ним ведется своеобразное тайное наблюдение. Полученная таким способом информация может использоваться для самых разнообразных целей. Это может быть относительно безобидный анализ посещаемости тех или иных сайтов, однако может быть и что-то противозаконное или наносящее ущерб пользователю.

Каким же образом шпионские модули проникают в компьютер? В большинстве случаев это происходит в процессе самостоятельной инсталляции пользователем нужных и полезных приложений. Например, существуют бесплатные программы, которые можно использовать только вместе со встроенной программой-шпионом. Если удалить это «дополнение», то основная программа работать не будет.

Кроме того, нужно внимательно относиться к установке программ: некоторые шпионы проникают в компьютер, например, после того, как пользователь, не задумываясь, утвердительно ответил на какой-либо запрос, который появился на экране в процессе инсталляции. Одни разработчики самостоятельно вставляют в дистрибутивы своих программ программы-шпионы, другие обращаются за помощью к фирмам, создающим и поставляющим подобные приложения. Кроме этого, программы-шпионы могут проникать в компьютер из Интернета.

Виды шпионских модулей

В настоящее время особенно распространены следующие виды шпионских модулей.

- Сканер жесткого диска. Такие модули изучают содержимое жесткого диска и отправляют данные по указанному адресу. В результате злоумышленник получает информацию об установленных на компьютере программах, хранящихся файлах и т. п.
- Клавиатурный шпион. Подобные программы постоянно наблюдают за клавиатурой и запоминают нажатие каждой клавиши, после чего отправляют эти данные по указанному адресу. В результате вся набранная информация попадает к посторонним лицам; а ведь это могут быть и письма, и секретные документы, и, что еще хуже, пароли, номера кредитных карт и т. п. Более подробно о клавиатурных шпионах рассказано ниже.
- Автоматический дозвон. При внедрении на компьютер такой программы модем будет автоматически устанавливать соединение с указанным в ней телефонным номером. Поскольку в большинстве случаев этот номер находится в отдаленной стране, то пользователь рискует получить астрономический телефонный счет. Чтобы защититься от подобных неприятностей, рекомендуется держать включенным динамик модема. В этом случае вы наверняка обратите внимание на то, что модем самостоятельно набирает какой-то телефонный номер.
- Контролер программ. Шпионы этого вида собирают и отправляют по определенному адресу информацию о наиболее часто используемых на данном компьютере программах.
- Почтовый шпион. Эти программы «вносят коррективы» в почтовые сообщения: например, они могут изменять подпись

в электронных письмах, вставлять в них рекламную информацию и др. Некоторые почтовые шпионы передают злоумышленникам содержимое адресной книги и информацию об активном почтовом ящике. Такие данные ценятся среди спамеров.

- Программы типа «прокси-сервер». Компьютер с такой внедренной программой легко использовать в качестве прокси-сервера для работы в Интернете. Злоумышленник, который установил такую программу на компьютер, как бы прикрывается чужим именем: ответственность за все его действия (как законные, так и незаконные) ложится на пользователя зараженного компьютера.
- Интернет-монитор. Подобные шпионы собирают информацию о работе пользователя в Интернете — в частности, о посещаемых страницах, совершаемых заказах и покупках и т. п. Некоторые из таких программ наряду с другой информацией успешно запоминают, например, номера кредитных карточек, используемых при расчетах за товары интернет-магазинов.
- Прочие шпионские модули. К этому виду можно отнести комбинированные программы-шпионы, например сканер жесткого диска, совмещенный с контролером программ.

  Здесь также можно отметить бессмысленные, шутливые программы-шпионы. Как правило, они не передают никому информацию, не ведут никакого наблюдения, а просто периодически выдают на экран сообщения о каких-либо несуществующих неполадках (например, Ваш компьютер заражен вирусом; через 15 минут начнется автоматическое форматирование диска C). Не исключено, что, прочитав подобное сообщение, испуганный пользователь начнет лихорадочно сохранять всю более-менее ценную информацию на внешние носители да и вообще совершать массу ненужных действий. Возможно также, что, не дождавшись обещанного форматирования диска, пользователь сам запустит этот процесс — как говорится, «от греха подальше» (разумеется, это относится в первую очередь к неопытным пользователям).

Борьба со шпионскими модулями

Характерной особенностью шпионских модулей Spyware является то, что их трудно распознать с помощью штатных антивирусных

программ. Поэтому для борьбы с ними рекомендуется использовать специальные утилиты, которые во множестве представлены в Интернете. Однако при этом обязательно нужно учитывать следующее: многие шпионские программы искусно маскируются именно под утилиты для борьбы с ними. Иначе говоря, установив на свой компьютер утилиту для борьбы с Spyware, можно вместо нее заполучить сам шпионский модуль. Поэтому для распознавания и устранения Spyware лучше использовать утилиты известных разработчиков или прислушаться к рекомендациям других пользователей, столкнувшихся с подобной проблемой ранее.

Может ли пользователь самостоятельно (без применения специальных утилит) заметить присутствие в компьютере шпионской программы? Да, в некоторых случаях это возможно. Перечислю наиболее характерные симптомы, свидетельствующие о проникновении в систему программы-шпиона (некоторые из этих признаков относятся также к рекламным модулям Adware, рассмотренным далее):

- при запуске Internet Explorer по умолчанию начинает открываться совершенно незнакомая веб-страница вместо пустой или заданной в качестве домашней;
- значительно увеличивается исходящий трафик;
- сбои в работе операционной системы;
- неоправданно высокие счета за телефонную связь (в таком случае в компьютер наверняка проник шпионский модуль автоматического дозвона);
- в Internet Explorer присутствуют незнакомые элементы управления (кнопка, пункт контекстного меню, инструментальная панель и т. п.);
- незнакомые пункты в списке Избранное, удалить которые невозможно;
- в окне Диспетчера задач на вкладке Процессы видно, что какой-то новый процесс использует практически все ресурсы компьютера;
- на экране монитора периодически появляются рекламные окна, причем даже при отсутствии действующего подключения к Интернету;
- на Рабочем столе появляются незнакомые значки, после щелчка на которых вы автоматически переходите на незнакомую веб-страницу.

Кроме этого, для обнаружения Spyware можно провести небольшую «ревизию» содержимого компьютера. В частности, следует проверить содержимое папки Program Files, каталога автозагрузки, а также раздела Установка и удаление программ на Панели управления. Некоторые шпионские программы помещают свой значок в область уведомлений Панели задач, поэтому при возникновении подозрений нужно проверить, не появился ли там неизвестный значок. Необходимо также проверить содержимое подменю Пуск ▸ Все программы — некоторые шпионские модули могут проявиться здесь. В Internet Explorer следует обратить внимание на страницу, открывающуюся по умолчанию, а также на содержимое папки Избранное.

Далее кратко рассмотрим несколько популярных утилит, специально предназначенных для поиска и удаления шпионских модулей. Учтите, что каждую из них необходимо периодически обновлять — по аналогии с антивирусными программами.

Microsoft Antispyware. Данная утилита корпорации Microsoft является популярной программой для борьбы со шпионскими модулями. Она работает с операционными системами Windows 2000, Windows XP и Windows 2003 Server. Эту программу можно бесплатно скачать с сайта Microsoft и из других источников в Интернете. Однако следует учитывать, что размер дистрибутива, предлагаемого к скачиванию, достаточно велик — около 6,5 Мбайт.

К достоинствам данной программы можно отнести успешное блокирование практически любых шпионских модулей, которые пытаются проникнуть в компьютер. Поэтому использование Microsoft Antispyware при работе в Интернете позволяет чувствовать себя в относительной безопасности. «Слабое место» программы — сканирование компьютера на наличие Spyware. Если компьютер заражен шпионскими модулями, то Microsoft Antispyware не всегда успешно обнаруживает их (особенно это касается малознакомых шпионских модулей).

SpywareBlaster. Программа SpywareBlaster, разработчиком которой является фирма Javacool Software, обеспечивает достаточно надежную защиту от различных шпионских модулей. Для домашнего использования эта утилита распространяется бесплатно, и ее можно без труда найти в Интернете. Размер дистрибутива, предлагаемого к скачиванию, примерно равен 2,5 Мбайт. Данная программа предназначена для работы с операционной системой Windows любой версии начиная с Windows 95.

SpywareBlaster отличается эргономичным, простым и интуитивно понятным пользовательским интерфейсом, в котором большинство параметров можно настроить с помощью флажков и переключателей. Среди всего многообразия параметров следует обратить внимание на возможность блокирования настроек домашней страницы, после которого ни один шпионский модуль не сможет изменить, например, адрес страницы, загружаемой по умолчанию. В программе также реализована возможность отката настроек браузера.

Данная утилита может работать не только с Internet Explorer, но и с другими популярными интернет-обозревателями — Netscape, Mozilla и др. Исключение составляет только браузер Opera.

Просто зафиксируйте настройки браузера (причем можно сохранить несколько различных конфигураций настроек) — и вы сможете вернуться к ним в любой момент. Например, к сохраненным параметрам можно вернуться при возникновении подозрений, что в настройки обозревателя без вашего участия внесены нежелательные изменения.

Кроме того, программа SpywareBlaster имеет еще множество интересных возможностей.

AVZ. Еще одна полезная утилита для борьбы с «компьютерным мусором» — программа AVZ, которая также распространяется бесплатно. Многие пользователи считают ее одной из лучших программ для поиска и удаления не только программ-шпионов, но и различных рекламных модулей (подробно о рекламных модулях и методах борьбы с ними рассказывается в подразд. «Рекламные модули Adware и борьба с ними»). Кстати, помимо шпионских и рекламных модулей, эта программа успешно борется с некоторыми вирусами.

Русскоязычный интерфейс программы прост и понятен пользователю. Основные параметры настройки сгруппированы на трех вкладках: Область поиска, Типы файлов и Параметры поиска. Вы можете задать программе, как поступать при обнаружении вредоносного объекта конкретного типа (вирус, программа-шпион и др.): удалять, просто информировать соответствующим сообщением и т. д. Кроме этого, можно настроить сканирование на выборочный поиск вредоносных программ: например, искать и удалять только шпионские модули, а все остальное игнорировать.

В нижней части окна ведется протокол процесса сканирования. Полученный результат при необходимости можно сохранить в отдельном файле для последующего изучения.

Клавиатурные шпионы

Несмотря на то что в подразд. «Шпионские модули Spyware и борьба с ними» уже упоминалось о клавиатурных шпионах, на них следует остановиться подробнее. В первую очередь это обусловлено тем, что клавиатурные шпионы являются чуть ли не самыми коварными из всего многообразия шпионских модулей и программ.

Клавиатурный шпион — это программа или устройство, постоянно наблюдающее за нажатием клавиш на клавиатуре, а иногда также за щелчками кнопками мыши с целью получения информации обо всех действиях пользователя. Зачем это нужно? Ответ на данный вопрос у каждого злоумышленника свой: одному нужно перехватить почтовые сообщения, другому — получить номера кредитных карт, третьему — взломать пароли, четвертому — украсть у разработчика исходные тексты еще не вышедшей программы, а пятому — все перечисленное и еще что-нибудь.

Характерной особенностью клавиатурных шпионов является то, что это может быть не только внедренное в компьютер вредоносное программное обеспечение, но и отдельное устройство. Такие устройства могут быть установлены между клавиатурой и системным блоком и достаточно долго оставаться незамеченными из-за своих небольших размеров. Однако чтобы установить такое устройство, необходимо получить доступ к компьютеру в отсутствие пользователя, поэтому на домашних компьютерах такой вид клавиатурных шпионов встречается редко. Чаще эти устройства подключаются к рабочим компьютерам, а также к компьютерам «общественного пользования»: в студенческих аудиториях, на почтах, в интернет-клубах и др. Чтобы своевременно обнаружить такой «сюрприз», рекомендуется почаще обращать внимание, не появилось ли между клавиатурой и системным блоком неизвестное устройство.

Достаточно широко распространены так называемые перехватывающие клавиатурные шпионы. Такие шпионы чаще всего представляют собой программы, состоящие из исполняемого файла с расширением EXE и DLL-библиотеки, с помощью которой осуществляется управление процессами записи информации. Перехватывающий клавиатурный шпион без проблем запоминает практически любой набранный текст: документы, письма, исходные коды программ (данная возможность нередко используется для кражи еще не вышедших программ), номера кредитных карт, пароли (в том числе и самозаполняющиеся) и т. д.

Клавиатурный шпион-программа может проникнуть в компьютер разными способами: например, как и любой другой шпионский модуль, в составе устанавливаемой на компьютер бесплатной программы (как правило, неизвестного или сомнительного разработчика), через программу обмена сообщениями и т. д. В последнее время клавиатурные шпионы все чаще попадают в компьютер после посещения пользователем определенного сайта.

Итак, рассмотрим следующие вопросы:

- как предупредить проникновение клавиатурных шпионов в компьютер;
- как попытаться обмануть такого шпиона, если он, возможно, уже проник в компьютер (меры предосторожности при вводе секретных данных);
- как обнаружить и удалить программу-шпиона.

В первую очередь отмечу, что стопроцентной защиты от клавиатурных шпионов, как и от других вредоносных программ, в настоящее время не существует: как известно, на каждое противоядие можно найти новый яд. Однако вы можете свести к минимуму вероятность их проникновения в компьютер, соблюдая некоторые меры предосторожности.

Для защиты от аппаратных клавиатурных шпионов рекомендуется по возможности ограничить доступ посторонних лиц к компьютеру. В первую очередь это касается компьютеров, установленных на рабочих местах (разумеется, при этом не следует впадать в крайности и отгонять от компьютера, например, системного администратора). Кроме того, как уже упоминалось, необходимо периодически проверять, не появилось ли между клавиатурой и системным блоком какое-либо неизвестное устройство. Иногда это касается и домашнего компьютера: вспомните, кто имеет к нему доступ? Одно дело — если только вы, и другое — если, например, к вашему сыну-студенту периодически приходят друзья-компьютерщики. В последнем случае, потехи ради или с более серьезными намерениями, вам вполне могут подсунуть какого-нибудь «жучка».

Что касается программных шпионов-перехватчиков, то для защиты от них можно применять меры, перечисленные в подразд. «Как предостеречь компьютер от вредоносных программ».

Что же делать, если вы предполагаете, что в компьютер проник клавиатурный шпион? Конечно, в первую очередь необходимо ска-

нировать компьютер специальной программой. Для поиска и уничтожения клавиатурных шпионов можно использовать некоторые программы, предназначенные для борьбы с другими Spyware. Кроме этого, есть программы, специально разработанные для поиска и избавления от клавиатурных шпионов (одну из таких программ рассмотрим чуть ниже). Однако бывают ситуации, когда немедленно сканировать компьютер невозможно и в то же время необходимо срочно выполнить какие-либо действия с конфиденциальными данными. Как же поступить в таком случае?

При возникновении подобных ситуаций рекомендуется использовать так называемую виртуальную клавиатуру. Виртуальная клавиатура — это программа, интерфейс которой представляет собой изображение клавиатуры. Нужные символы в этом случае вводят с помощью мыши. Поскольку принцип действия большинства клавиатурных шпионов заключается в перехвате вводимых с клавиатуры символов, то использование виртуальной клавиатуры достаточно эффективно.

Однако необходимо учитывать, что некоторые клавиатурные шпионы снимают копии экрана после каждого щелчка кнопкой мыши. Для защиты от таких шпионов предусмотрены виртуальные клавиатуры, в которых для ввода символа достаточно просто подвести указатель мыши к соответствующей позиции. Благодаря этому можно ввести информацию без единого щелчка.

При частой или регулярной работе с конфиденциальными данными рекомендуется постоянно использовать виртуальную клавиатуру: никогда нельзя полностью быть уверенным в том, что в компьютер не проник клавиатурный шпион.

Как упоминалось, для уничтожения клавиатурных шпионов можно использовать программы, предназначенные для борьбы с другими Spyware, а также специальные приложения. Одной из таких специальных программ является Anti-keylogger, разработанная российскими специалистами. Скачать демонстрационную версию данной программы можно в Интернете по адресу: http://dl.softportal.com/load/antikey.zip. Размер дистрибутива — 3,29 Мбайт.

К достоинствам программы можно отнести ее многоязычность (она поддерживает русский, английский, немецкий, французский и украинский языки); к недостаткам — относительно высокую стоимость (полнофункциональная версия программы стоит чуть менее $60).

Характерной особенностью программы Anti-keylogger является то, что при работе она не использует сигнатурные базы. Это позволяет ей выявлять и блокировать любые виды клавиатурных шпионов: как известные большинству аналогичных программ, так и не известные.

Программа обладает простым и дружественным пользовательским интерфейсом. В разделе Опции предусмотрена возможность настройки параметров работы программы. Кроме этого, в разделе Лист исключений реализована возможность ведения списка исключений; в этот список можно включать программы, которые не должны распознаваться как клавиатурные шпионы.

Помимо Anti-keylogger, в Интернете можно найти еще множество программ (как платных, так и бесплатных), специально предназначенных для борьбы с клавиатурными шпионами.

Как получить пользу от Spyware

Как ни парадоксально, из некоторых шпионских модулей и программ можно извлечь определенную пользу, и это нередко практикуется. Итак, программы-шпионы могут быть полезны следующим категориям людей.

- Руководителям предприятий и организаций. Внедрив на компьютеры подчиненных какую-либо шпионскую программу, можно достаточно успешно контролировать то, чем занимаются сотрудники в рабочее время. Можно узнать, какой текст они набирают, когда открывают и закрывают различные программы, когда включают и выключают компьютер, что содержит буфер обмена и т. д. Некоторые программы-шпионы могут через определенные промежутки времени делать снимки экрана.
- Системным администраторам. С помощью программы-шпиона можно вести постоянное наблюдение за каждым пользователем и за действиями, которые он выполняет.
- Фискальным органам и силовым структурам. С помощью программ-шпионов можно получить необходимую оперативную информацию, которая поможет предотвратить планируемое преступление.
- Родителям. Установленная на компьютере программа-шпион позволит установить, что делал ребенок на компьютере: на-

пример, выполнял домашнее задание по информатике или играл. Большинству родителей интересно, какие ресурсы посещает их ребенок в Интернете — здесь также поможет программа-шпион.

- Рядовым пользователям. Если к компьютеру имеет доступ несколько человек, то с помощью программы-шпиона всегда можно узнать, какие действия выполнялись на компьютере в ваше отсутствие.

Кроме этого, следует отметить, что возможности многих программ-шпионов иногда позволяют восстанавливать утерянные данные: содержимое того или иного документа, пароль и т. п.

Рекламные модули Adware и борьба с ними

Наряду с вирусами, шпионскими программами и прочими раздражающими и вредоносными приложениями широкое распространение получили так называемые рекламные модули — Adware. В отличие от компьютерных вирусов, они, как правило, не причиняют ущерба хранящейся в компьютере информации. В большинстве случаев они не ведут также и шпионскую деятельность. Назначение таких программ — рекламирование различных товаров и услуг путем навязчивой демонстрации пользователям Интернета соответствующих баннеров, всплывающих окон, ссылок и т. п.

Откуда берутся Adware

Рекламные модули могут проникать в компьютер в процессе установки некоторых бесплатных программ. Иногда это является главным условием возможности работы с такой программой. Данный способ широко применялся для распространения первых Adware. Причем нередко в процессе инсталляции пользователю сообщалось о том, что такое Adware и с какой целью этот рекламный модуль включен в дистрибутив программы (например: Установка данного модуля является платой за использование программы). При инсталляции некоторых программ пользователю предлагалось выбрать вариант использования приложения: бесплатно с рекламным модулем Adware или на платной основе. Иногда при выборе платного варианта можно было в течение нескольких дней поработать с демонстрационной

версией программы. При деинсталляции программы одновременно удалялся и рекламный модуль.

Однако в настоящее время Adware практически не распространяются такими цивилизованными способами. Нередко рекламный модуль устанавливается на компьютер даже после того, как пользователь отказался от этого. Adware, проникший в компьютер, нелегко обнаружить и удалить (для этого нужно использовать специально разработанные утилиты, о которых рассказано ниже). Если рекламный модуль проник в компьютер в процессе инсталляции какой-либо программы, то при ее удалении уже и речи не идет о том, чтобы вместе с ней исчез рекламный модуль.

Рекламные модули, созданные с применением современных технологий, сравнимы с троянскими конями и иными вирусами. Они способны несанкционированно проникать в компьютер и вести там свою деятельность. Более того, некоторые Adware способны вступать в «схватки» с конкурентами, которые проникли в компьютер ранее, и уничтожать их. При этом часто бывает так, что пользователь ничего не подозревает об этих «сражениях» и иной бурной деятельности, которую ведут в компьютере рекламные модули. Только периодически появляющаяся реклама, с каждым разом раздражающая все сильнее, может навести на мысли, что в компьютере «кто-то поселился».

Каким же образом действуют рекламные модули? Все зависит от их направленности, а также от фантазии разработчика. Например, очень раздражает пользователей появление рекламных всплывающих окон. Как правило, такие окна появляются именно тогда, когда их хочется видеть меньше всего. Созданные с применением передовых технологий рекламные всплывающие окна трудно убрать с экрана. Нередко они даже перемещаются по странице при прокрутке ее содержимого, оставаясь перед глазами пользователя.

Разновидностью рекламных всплывающих окон являются переходные и дополнительные окна. Переходные окна появляются после щелчка на какой-либо ссылке и отображаются до открытия следующего окна, а дополнительные возникают между двумя информационными окнами.

Одним из видов навязчивой рекламы является автоматическое размножение окон браузера. В каждом окне при этом загружается определенная веб-страница.

Некоторые рекламные модули выводят на экран рекламу, которую невозможно убрать с помощью кнопок Назад или Закрыть, по-

скольку эти кнопки оказываются заблокированными. В данном случае закрыть окно с рекламой можно только нажатием сочетания клавиш Alt+F4 или снятием соответствующей задачи в окне Диспетчера задач.

Неприятной особенностью многих Adware является то, что реклама на экране может появляться даже при отсутствии действующего подключения к Интернету.

Способы борьбы с рекламными модулями

Рекламные модули Adware, как и шпионские программы Spyware, трудно обнаружить и уничтожить с помощью штатных антивирусных программ. Несмотря на то что некоторые разработчики антивирусного программного обеспечения включают в свои продукты функции для борьбы с рекламными модулями, целесообразнее использовать для этого специальные утилиты, которые во множестве представлены в Интернете. Рассмотрим некоторые из них. Отмечу, что большинство утилит предназначено для поиска и удаления не только рекламных модулей, но и других вредоносных программ.

Spyware Annihilator Pro. Программа Spyware Annihilator Pro, разработчиком которой является компания Solidlabs Technology, предназначена для поиска и устранения шпионских и рекламных модулей. К достоинствам программы можно отнести возможность использования русскоязычного интерфейса, а также то, что размер дистрибутива, предлагаемого к скачиванию (его можно легко найти в Интернете), достаточно невелик — около 330 Кбайт. Данная программа является платной, но вы можете поработать с бесплатной демонстрационной версией.

Возможности программы предусматривают сканирование следующих объектов: оперативной памяти, системного реестра (причем реестр можно сканировать в двух режимах: Бегло и Основательно), файлов Cookies, а также локальных, сетевых дисков и дискет. Для выбора объектов сканирования достаточно установить соответствующие флажки.

Интерфейс программы достаточно прост, поэтому настроить требуемые параметры и проверить компьютер сможет даже начинающий пользователь. Однако следует учитывать, что удалить обнаруженные шпионские и рекламные модули вы сможете только после оплаты программы (демонстрационная версия только ищет вредоносные программы, но не удаляет их).

Ad-Aware. Полифункциональная программа Ad-Aware, разработчиком которой является немецкая компания Lavasoft, представляет собой мощную утилиту для обнаружения и удаления вредоносных программ различных типов, в том числе рекламных модулей. Следует отметить, что в настоящее время Ad-Aware является одной из самых популярных программ подобного рода. Достоинством данной программы является наличие бесплатной версии, единственное ограничение которой — отсутствие защиты компьютера в режиме мониторинга. Немаловажным является и то, что в программе реализована возможность использования русскоязычного интерфейса. Размер дистрибутива программы, предлагаемого для скачивания, — 1,7 Мбайт.

В процессе сканирования Ad-Aware проверяет содержимое оперативной памяти, системного реестра, а также настройки и содержимое Internet Explorer.

Утилита отличается простым, эргономичным и дружественным интерфейсом, что делает работу с ней доступной даже начинающим пользователям.

NoAdware. Данная утилита помогает избавиться не только от рекламных модулей, но и от множества других вредоносных программ. Размер дистрибутива последней версии программы (NoAdware 4.0), предлагаемого для скачивания, составляет примерно 980 Кбайт.

К достоинствам программы можно отнести ее быстродействие и простоту в использовании; к недостаткам — отсутствие русскоязычного интерфейса.

В процессе сканирования программа проверяет системный реестр и локальные диски компьютера. При необходимости можно выборочно проверить только объекты, вызывающие подозрение. В программе реализована возможность ручного или автоматического обновления базы.

Spybot — Search & Destroy. Основное предназначение данной программы — поиск и уничтожение шпионских и рекламных модулей, проникших в компьютер. Кроме этого, в ней реализована возможность очистки временных файлов Интернета и Cookies, а также удаления информации о предыдущем использовании компьютера. Несомненные достоинства этой утилиты — бесплатное распространение и мультиязычность (предусмотрено использование более 30 языков, в том числе русского).

В программе заложена возможность гибкой настройки параметров сканирования. В частности, можно установить выборочное ска-

нирование: например, искать только рекламные модули Adware, а шпионские модули и прочие вредоносные программы игнорировать. Кроме этого, средства программы позволяют запомнить состояние настроек системы, а затем при необходимости (для устранения последствий пребывания вредоносных программ) выполнить откат к сохраненному состоянию.

Следует отметить возможность программы отслеживать загружаемые из Интернета файлы, что позволяет выявить вредоносные модули еще до проникновения их в компьютер.

4. Чем опасен Интернет

Трудно переоценить роль, которую играет Интернет в жизни современного человека. Знание Интернета и умение работать с ним предоставляют пользователям массу преимуществ и удобств. С каждым днем растет количество людей, открывших для себя Всемирную сеть, и очевидно, что в обозримом будущем это количество будет только увеличиваться.

Однако Интернет может приносить не только пользу. Не имея определенных навыков работы в Сети и не соблюдая необходимые меры предосторожности, можно стать жертвой Интернета. Потеря ценной информации, выход компьютера из строя, утрата денежных средств и даже ответственность за несовершенные противозаконные действия — это далеко не все проблемы и неприятности, которыми чревато неумелое обращение с Интернетом.

Даже обладая определенными навыками и опытом работы в Интернете, нельзя полностью чувствовать себя в безопасности. В первую очередь это обусловлено тем, что многочисленные злоумышленники из самых разных уголков земного шара постоянно выбрасывают в Сеть новые вирусы, троянских коней, программы-шпионы, совершают хакерские атаки и прочие несанкционированные действия, от последствий которых не застрахован ни один пользователь. Однако каждому вполне по силам свести возможные неприятности к минимуму.

Из этой главы вы узнаете о мерах предосторожности, которые необходимо соблюдать, находясь в Интернете, и некоторых популярных способах интернет-мошенничества. Вы также познакомитесь с программами, с помощью которых можно полностью закрыть свой компьютер от любого постороннего доступа.

Правила поведения в Сети

Чтобы максимально обезопасить себя от возможных неприятных сюрпризов, которыми наполнен Интернет, надо соблюдать следующие меры предосторожности.

- Необходимо установить на компьютер хорошую антивирусную программу и включить в ней режим постоянного мониторинга. В таком случае вы сможете выявлять опасность сразу после ее возникновения. Некоторые популярные антивирусы рассмотрены в подразд. «Лучшие антивирусные программы».
- При посещении неизвестных ресурсов в Интернете следует соблюдать предельную осторожность. В настоящее время широкое распространение получили вирусы и вредоносные программы, для заражения которыми достаточно просто посетить определенную веб-страницу.
- Динамик модема должен быть включен. Это позволит своевременно обнаружить попытки сетевых злоумышленников подключить ваш компьютер к некоему ресурсу путем набора заданного телефонного номера (часто это практикуют распространители порнографических сайтов и услуг аналогичного характера). Если при работе за компьютером слышно, что модем начал произвольно набирать какой-то номер без вашего участия, немедленно отключитесь от Интернета путем отсоединения сетевого кабеля. После этого нужно проверить компьютер специальной программой типа Antispyware (описание некоторых подобных программ приведено выше): скорее всего, в компьютер внедрен шпионский модуль автоматического дозвона.
- После скачивания из Интернета файлов, архивов, а также прочих объектов необходимо проверить их антивирусной программой и лишь после этого запускать, распаковывать и т. д. Многие вирусы и вредоносные программы представляют собой исполняемый файл или архив.
- Почтовые письма, получаемые от неизвестных и сомнительных отправителей, перед открытием нужно обязательно проверять хорошей антивирусной программой с обновленными базами. Если этого не делать, можно в короткие сроки превратить свой компьютер в рассадник вирусов.
- Любители виртуального секса (например, с использованием веб-камеры) должны иметь в виду, что видеофильмы с их изображением могут появиться на различных порносайтах. По этой же причине не стоит выкладывать в Интернете свои неприличные фотографии.

- Ни в коем случае нельзя отвечать на письма, содержащие просьбу прислать конфиденциальные данные (имя пользователя, пароль и т. п.) по указанному адресу. С помощью такого нехитрого приема злоумышленники завладевают чужими именами и паролями.
- Не стоит отвечать на письма, которые являются спамом. В противном случае спамер будет знать, что ваш почтовый ящик действителен, и в результате количество получаемого спама многократно увеличится.
- Если при посещении различных ресурсов Интернета (форумов, порталов, сайтов и т. д.) требуется оставить о себе некоторые данные, то такая информация должна быть минимальна (например, совершенно необязательно сообщать свои паспортные данные, домашний адрес, различные пароли и т. п.). Несмотря на то что в большинстве подобных случаев вам гарантируют полную конфиденциальность, не стоит быть наивным: если кому-то нужно получить эту информацию, то он ее получит. Варианты утечки информации могут быть самыми разными, и конфиденциальную информацию могут получить следующие типы пользователей.
  - Хакер. Он просто взломает систему защиты сайта или портала (или сотворит нечто подобное).
  - Шантажист. Если кто-то заводит в Интернете различные фривольные знакомства, указывая при этом в качестве средства связи номер телефона или адрес основного почтового ящика, то по этим данным с использованием широких возможностей современных мощных поисковых систем можно легко собрать на человека компромат.
  - Лицо (или группа лиц), собирающее о людях информацию индивидуального характера, например паспортные данные. В этом случае заинтересован (а чаще всего — подкуплен) сотрудник портала, имеющий доступ к этим данным. В результате беспечный пользователь через некоторое время узнает, причем, как правило, от правоохранительных органов, что, например, на его паспортные данные открыта оффшорная (или еще какая-нибудь) фирма, через которую каждый день «отмывается» десяток-другой миллионов долларов. Нетрудно догадаться, что ответственность за это ляжет именно на

пользователя, который легкомысленно доверил свои личные данные администрации интернет-ресурса.

- Представитель известных силовых структур. Он просто свяжется с администрацией сайта (портала) и вежливо попросит предоставить ему всю информацию о зарегистрировавшихся на сайте пользователях (и, разумеется, получит ее в кратчайшие сроки).

■ После окончания работы в Интернете следует обязательно отключить сетевой кабель от телефонной линии.

Помимо перечисленных правил безопасности, при работе в Интернете следует руководствоваться также правилами, существование которых диктуется здравым смыслом и общими правилами хорошего тона.

Схемы выманивания денег через Интернет

Одним из наиболее распространенных видов интернет-мошенничества является выманивание денег у пользователей.

В настоящее время выманивание денег через Интернет приобрело такие масштабы, что описанию используемых для этого схем можно посвятить отдельную книгу. С каждым днем интернет-мошенники совершенствуют свое мастерство, принося финансовый урон миллионам пользователей во всем мире. В этом разделе вы узнаете о некоторых наиболее популярных и распространенных схемах выманивания денег через Интернет.

В первую очередь, отмечу, что принцип у большинства таких схем одинаков: пользователю предлагается быстрое и сказочное обогащение, которое не требует практически никакого участия. Единственное условие — необходимо перевести некоторую сумму денег по указанным реквизитам, после чего доходы потекут рекой. «Это классическое правило бизнеса: чтобы получить доход, нужно сделать определенные вложения!» — завлекают «благодетели». Разумеется, после перевода денег пользователь в лучшем случае получает какие-нибудь бессмысленные инструкции, а в чаще всего таинственный «благодетель» просто исчезает, не отвечая на письма (разумеется, не сообщив ни телефон, ни адрес проживания).

Итак, рассмотрим подробнее некоторые популярные схемы выманивания денег.

«Грабь награбленное», или «Нигерийский спам»

«Нигерийский спам» — это схема выманивания денег, при которой пользователь получает письмо примерно следующего содержания.

Я, такой-то, недавно работал секретарем Саддама Хусейна (варианты — «черным» кассиром Ясира Арафата, финансовым работником Бориса Березовского, в последнее время очень популярны такие письма от «бухгалтеров», «финансовых директоров» и т. п. компании «ЮКОС»), *и мне удалось завладеть суммой 50 млн долларов США* (разумеется, суммы фигурируют самые разные). *Но самостоятельно я их снять не могу* (в силу каких-то причин), *и мне нужна помощь постороннего лица. Вы можете мне помочь. Для этого вам нужно открыть счет в зарубежном банке, на который будут перечислены денежные средства. За это вам причитается 5 %* (или 1 %, или 20 %) *от суммы.*

Затем пользователю предлагается перечислить некоторую сумму денег для покрытия «накладных расходов». Само собой, после перечисления «накладных расходов» никакая «помощь» от пользователя уже не требуется.

История возникновения денег может быть разной: не только «мне удалось завладеть деньгами бывшего шефа», но и, например, «помогите спасти часть капитала (эдак $ 500 млн) бывшему олигарху, попавшему в беду... для этого откройте счет... причитается вознаграждение... небольшие накладные расходы...». В последнее время в таких письмах часто используется имя Михаила Ходорковского.

Почему этот вид мошенничества получил название «нигерийский спам»? Дело в том, что в первых подобных письмах, которые рассылались по всему миру, фигурировало имя бывшего нигерийского диктатора Сани Абачи (якобы люди, имеющие доступ к его счетам, не могли снять деньги без посторонней помощи). В настоящее время в таких письмах можно встретить имена любых известных людей (чаще всего — попавших в неприятность, например преследуемых официальными властями или вообще умерших), но первоначальное название так и осталось.

Оплата хакерских услуг

В качестве «приманки» для вытягивания денег пользователя могут предлагать различные хакерские услуги. Наиболее распространенные — взлом почтовых ящиков, подбор паролей, раскрутка сайта и т. п. Например, какой пользователь откажется от возможно-

сти просмотреть содержимое почтового ящика своего начальника? Или конкурента? Или жены? Вариантов заинтересовать доверчивого пользователя более чем достаточно. Все это удовольствие — всего за 30 (сумма может быть любой) долларов США! После перевода денег пользователь будет долго и безнадежно ждать оплаченной информации...

Стоит также упомянуть о мнимых «раскрутках» сайтов. Каждый владелец сайта желает, чтобы у него было много посетителей. Чтобы отслеживать их количество, на сайт устанавливают специальные счетчики (в Интернете представлено большое количество таких счетчиков). Если на сайт заходит достаточно большое количество посетителей, то с этого можно получить определенную выгоду: например, разместить на нем платную рекламу. Именно это толкает многих владельцев сайтов в сети мошенников.

Многие пользователи видели в Интернете массу объявлений типа: «Раскрутка сайта в короткие сроки — дешево и качественно». Причем зачастую предоплата за такие услуги не требуется. Человек заказывает раскрутку сайта и уже через некоторое время видит результат: количество посетителей сайта растет в геометрической прогрессии. Разумеется, он оплачивает услуги раскрутки, полагая, что его сайту в Интернете сделана мощная реклама и от посетителей теперь не будет отбоя. Однако сразу после оплаты услуг по раскрутке количество посетителей резко снижается и остается примерно на уровне, который был до действий «доброжелателя». Секрет прост: никто никакой рекламой и раскруткой сайта не занимался, а счетчик искусственно «накручивался» путем нехитрых манипуляций.

Финансовые интернет-пирамиды

Схема финансовых пирамид многим знакома из реальной жизни. У многих еще на слуху печально известные АО «МММ», «Хопер-Инвест», «Русский дом Селенга» и т. п. Аналогичный механизм в настоящее время успешно используется многими интернет-мошенниками.

Обычно предложение поучаствовать в финансовой пирамиде приходит в виде спамерского письма. Кроме этого, реклама подобных мероприятий часто встречается на страницах Интернета. Пользователю предлагается внести определенный взнос под умопомрачительные проценты и ждать баснословных барышей. При этом никаких гарантий на руки вообще не выдается (кстати, «МММ»

и ему подобные хоть акции выдавали...). На словах, конечно, сообщается, что сохранность вклада и получение процентов гарантируется всеми, кем только можно (хоть правительством, хоть папой римским).

Как ни странно, в наше время еще находятся люди, готовые перечислить свои денежки «под честное слово» неизвестно кому для участия в сомнительном проекте. Поэтому данный вид мошенничества все еще достаточно распространен.

«Волшебный кошелек»

С каждым днем растет популярность различных платежных интернет-систем, наиболее известными из которых являются системы Web Money и «Яндекс. Деньги». Несомненно, использование таких систем весьма удобно, например, для оперативных расчетов за товары, услуги, выполненные работы и т. д. Росту популярности платежных интернет-систем способствует и то, что они позволяют совершать денежные расчеты втайне от налоговых и других подобных органов. Поэтому нет ничего удивительного в том, что интернет-мошенники не оставили их без внимания. Приведу распространенный способ выманивания денег из чужих кошельков.

«Приманка» обычно забрасывается с помощью спамерского письма или объявления, которое размещается на многочисленных досках бесплатных объявлений в Интернете. Содержимое письма или объявления примерно такое.

Добрый день! Я долгое время работал в службе техподдержки (отделе разработки и т. п.) *компании Web Money* (или «Яндекс. Деньги» и т. п.). *Недавно меня незаслуженно уволили. Но перед увольнением я сумел украсть секрет. Если перевести деньги на специальный кошелек* (или несколько кошельков), *то максимум через три дня они вернутся к вам в трехкратном* (пятикратном, десятикратном — возможны варианты) *размере. Вот его номер: №№№. Спешите увеличить свой капитал! Время ограничено! Удачи!*

Думаю, не стоит объяснять, что это всего-навсего наглый, примитивный обман и никаких «волшебных кошельков» не существует. На эту удочку иногда попадаются пользователи, которые недавно установили себе платежную интернет-систему, толком не уяснили ее возможности и поэтому верят в подобные небылицы.

Службы Web Money и других платежных систем отслеживают и оперативно уничтожают такие «кошельки» вместе со всем содержимым.

Следует упомянуть о программах, которые якобы позволяют путем взлома паролей получить доступ к чужим кошелькам Web Money и других платежных систем, ключей и т. п. Большое количество таких программ продается в Интернете. Эти программы объединяет то, что в настоящее время ни одна из них не способна взломать чужой кошелек.

«Устройство на работу»

В настоящее время многие ищут работу или приработок с помощью Интернета. Это очень удобно: можно подать объявление и ждать результатов, не выходя из дома. Тем более что сайтов по данной тематике имеется великое множество. Само собой, без интернет-мошенничества здесь также не обошлось.

Одна из популярных схем выманивания денег выглядит так. Пользователь получает письмо, причем не обязательно спамерское: это может быть просто отзыв на оставленное резюме. В этом письме красочно описываются сказочные перспективы: «Я был почти нищим, весь в долгах, но благодаря этой замечательной программе быстро разбогател... теперь у меня много денег, вилла на Канарах, несколько машин...» — и тому подобная ерунда. Причем это описание достаточно длинное, может занимать несколько страниц. Короче говоря, пользователя, получившего письмо, сначала «обрабатывают» по полной программе.

Если человек, получивший такое предложение, недостаточно опытный, то он не удалит письмо сразу, как стоило бы сделать, а дочитает до конца. Вот в конце-то и будет сказано о главном условии подобного «счастья»: нужно всего-навсего перевести по указанным реквизитам (чаще всего — на кошелек WebMoney или аналогичной платежной системы) некоторую сумму денег (от $10 до бесконечности). Причем не просто перевести, а оплатить какой-либо информационный пакет, или ключ, или инструкции, или еще что-нибудь, необходимое для дальнейшей «работы». Нужно сказать, что в большинстве случаев после оплаты пользователь действительно получает по почте какую-то информацию, которая, правда, никаким положительным образом не отражается на его финансовом благополучии. Чаще всего это бессмысленные фразы типа «проявите усердие — и удача будет с вами».

Еще один способ выманивания денег заключается в том, что мошенник предлагает «содействие в трудоустройстве». Самый примитивный

вариант — предложение прислать свои данные вместе с некоторой суммой денег за «услуги по поиску работы», после чего ждать ответа. Само собой, ждать придется бесконечно.

Более «хитрый» вариант может выглядеть так. Пользователь получает отзыв на свое резюме, которое он разместил в Интернете. В письме сообщается, что его резюме заинтересовало руководство крупной (российской или зарубежной) компании. «Будущий работодатель» предлагает пройти удаленное тестирование, для чего необходимо заполнить анкету на сайте, ответить на присланные вопросы или еще что-то подобное. После этого придет письмо с содержанием типа «поздравляем вас, вы прошли предварительное тестирование, результаты отличные». В этом же письме (а может, в следующем) будет предложено продолжить тестирование, но для получения следующих вопросов (анкет и т. п.) нужно заплатить определенную сумму денег. Вот на этом этапе и нужно немедленно прекратить сотрудничество с «агентством», «работодателем» или как там еще мог представиться мошенник. В принципе, не исключено, что после оплаты пользователь получит еще какие-то тесты, анкеты или вопросы, но после их заполнения и отправки ответ будет или «к сожалению, повторное тестирование вы не прошли», или «вы успешно прошли тестирование, но пока вакансии для вас нет», или что-то аналогичное. В любом случае, если при поиске работы требуют деньги за содействие, за тестирование, за «бланки анкет» или за что-то еще, помните: это мошенничество.

Следует отметить, что агентства по трудоустройству, само собой, могут потребовать плату за свои услуги, но это ни в коем случае не предоплата (в данном случае «предоплата» и «мошенничество» — синонимы). Обычно плата за трудоустройство взимается в виде определенного процента с первой зарплаты соискателя, полученной им на новом месте работы, и этот процент строго оговаривается заранее.

Удаленное шифрование данных

В отличие от перечисленных схем выманивания денежных средств через Интернет, которые больше напоминают элементарное «кидалово», описанный в этом подразделе способ интернет-мошенничества относится к разряду «продвинутых» и требует от злоумышленника определенной квалификации.

Речь идет об удаленном шифровании данных. Его смысл заключается в том, что злоумышленник, получив доступ к удаленному компьютеру, шифрует в нем определенные файлы, документы или прочую информацию таким образом, что пользователь не может самостоятельно расшифровать их. Через определенное время пользователь зараженного компьютера получает электронное письмо с требованием перевести определенное количество денег (это может быть и $100, и 10 000, и любая другая сумма) по указанным реквизитам. За это ему будет предложено выслать ключ для расшифровки информации. Разумеется, в большинстве случаев пользователь готов отдать требуемую сумму, лишь бы вернуть зашифрованные данные.

Этот прием набирает в настоящее время все большую популярность. Следует отметить, что злоумышленники предпочитают шифровать данные, хранящиеся не на домашних (хотя нередки и такие случаи), а на корпоративных компьютерах и серверах. Это неудивительно: пользователь домашнего компьютера при всем желании не сможет заплатить столько же, сколько фирма, пусть даже небольшая.

При возникновении подобной ситуации можно считать удачей, если злоумышленник требует перевести деньги на банковский счет. В этом случае его относительно легко вычислить, своевременно обратившись в соответствующие органы. Если же в качестве платежных реквизитов указан кошелек Web Money, «Яндекс. Деньги» или аналогичной интернет-системы, то шансы обнаружить злоумышленника невелики. В этом случае самым лучшим итогом можно считать ситуацию, при которой после получения денег вам не поленятся выслать ключ для расшифровки данных.

Удаленное шифрование данных является одним из самых неприятных и опасных видов интернет-мошенничества.

Прочие способы выманивания денег

В данном подразделе кратко рассмотрим несколько других распространенных способов выманивания денег через Интернет.

Достаточно популярным является интернет-мошенничество, при котором вам предлагают найти «спутника жизни за границей». В России на эту удочку попадаются в основном потенциальные невесты, готовые заплатить деньги кому угодно, лишь бы выйти замуж за границу. За границей, наоборот, обманутыми в большинстве случаев

становятся мужчины, желающие найти себе русскую невесту. Известны случаи, когда один мошенник обманывал десятки и даже сотни людей. Он высылал им фотографии, вступал в переписку от имени «кандидата» и т. п. Затем он просил оплатить услуги или поступал еще проще: от имени избранника (избранницы) просил денег «на дорогу» или на что-нибудь подобное. Разумеется, после получения денег мошенник бесследно исчезал.

Аналогичным образом оказывают «содействие за умеренную плату» в решении множества других вопросов: выезд на постоянное место жительства за границу, получение гражданства, поступление в институт и т. п. В любом случае необходимо помнить: если кто-то требует перечислить через Интернет деньги в качестве предоплаты за оказанные услуги — скорее всего, это мошенничество.

Нередки случаи, когда мошенники прячутся под маской благотворительности. Например, они могут рассылать спамерские письма с просьбой «перечислить, сколько возможно, в фонд помощи пострадавшим от цунами» или «от урагана Катрина» и т. п. Характерной особенностью данного вида мошенничества является то, что в качестве «приманки» используется известное стихийное бедствие, имеющее широкий общественный резонанс. Иногда мошенники даже открывают сайты, посвященные этой теме. Такие сайты нередко содержат публикации известных благотворительных организаций с просьбой «помочь и поучаствовать», однако указанные платежные реквизиты не имеют к этим организациям никакого отношения.

Еще один популярный вид интернет-мошенничества — это различные интернет-казино, интернет-лотереи и т. п. Здесь для злоумышленников настоящее раздолье. Мало того, что мошенники открывают фиктивные казино и проводят вымышленные акции и лотереи, так они еще и продают различные «программы для выигрыша в интернет-казино». Стоит ли говорить, что такие «программы» — полнейшая фикция и ничего выиграть с их помощью не удастся.

Помимо перечисленных, в Интернете имеется много других способов выманивания денег у пользователей. Необходимо учитывать, что злоумышленники постоянно совершенствуют свое мастерство. Поэтому, встречая в Интернете разнообразные заманчивые предложения, необходимо помнить одно известное правило: бесплатный сыр бывает только в мышеловке.

Фишинг, или Кража данных о кредитных картах

Вид мошенничества, который рассмотрен в данном подразделе, используется для кражи информации о кредитных картах (номеров кредитной карты, пароля, пин-кода и т. д.) с целью присвоения хранящихся на них денежных средств.

Первые попытки фишинга были зафиксированы в конце 90 годов прошлого столетия. С тех пор популярность этого вида мошенничества постоянно растет.

Каким же образом мошенники могут заполучить информацию о чужой кредитной карте?

Наиболее распространен следующий способ. Пользователь получает электронное письмо, например от лица своего банка, с просьбой (а точнее, с требованием) срочно перейти по указанной в письме ссылке и подтвердить свои регистрационные данные. Ссылка приводит пользователя на поддельный сайт, который является точной копией сайта банка. Разумеется, ничего не подозревающий пользователь спокойно вводит конфиденциальные данные в форму на сайте, тем самым сообщая их злоумышленникам.

Необходимо учитывать, что возможны различные варианты подобного обмана. Например, мошенники могут попросить ввести регистрационные данные для подтверждения якобы полученного крупного денежного перевода.

Каким же образом распознать, что полученное от имени банка письмо является фальшивым?

В большинстве случаев подобные письма имеют следующие признаки:

- к пользователю обращаются не лично по имени и фамилии, а общим приветствием вроде: «Уважаемый клиент!»;
- в письме обязательно присутствует гиперссылка на сайт с предложением посетить его;
- требования подтвердить свои конфиденциальные данные весьма настойчивы;
- в письме могут быть угрозы типа «закрыть счет» или «прекратить сотрудничество» в случае отказа от выполнения требований;
- не исключено наличие в письме грамматических и иных ошибок.

Для заманивания пользователя на фальшивый сайт может также использоваться внедренная в его компьютер вредоносная программа. Задача этой программы заключается в том, чтобы автоматически перенаправить пользователя на фальшивый сайт, как только он наберет в строке браузера определенный веб-адрес (как правило, адрес своего банка). Ну а дальше — обычная схема: пользователь вводит конфиденциальные данные в предложенную форму, после чего они попадают в руки мошенников.

Иногда для фишинга используют специальные клавиатурные шпионы (подробно о таких вредоносных программах рассказано выше, в подразд. «Клавиатурные шпионы»). В отличие от обычных клавиатурных шпионов данные программы активизируются только после входа пользователя на определенный сайт (например, сайт банка). В результате все выполненные действия (в том числе и ввод данных о кредитной карте) становятся известны злоумышленникам.

Брандмауэр: непробиваемая стена

Помимо различных антивирусных и антишпионских программ, существует достаточно надежное средство, позволяющее защитить компьютер от несанкционированного доступа извне, — брандмауэр.

Брандмауэр (он может называться также «сетевой экран», «файрвол», «шлюз безопасности» и др.) — это своеобразный буфер, находящийся между локальным компьютером и Интернетом. Его задача — блокировать всяческие попытки проникновения различных программ, команд или заданий как из Интернета в компьютер, так и из компьютера в Интернет.

Может возникнуть вопрос: «Понятно, зачем брандмауэр блокирует несанкционированный доступ из Интернета в компьютер, но зачем же блокировать выход из компьютера в Интернет?» А затем, чтобы, например, троянский конь или иной шпион, проникший в компьютер до установки или включения брандмауэра, не смог выполнять полученное задание (рассылать с зараженного компьютера спам, отсылать информацию о компьютере и пользователе и т. п.). При этом выйти в Интернет смогут только те приложения, которые укажет пользователь (Internet Explorer, Outlook Express и т. п.). Следует, однако, отметить, что не все брандмауэры могут контролировать исходящий трафик.

В операционной системе Windows XP имеется встроенный брандмауэр подключения к Интернету. Чтобы включить брандмауэр, на Панели управления выберите категорию Сеть и подключения к Интернету, а затем щелкните на значке Сетевые подключения. В результате откроется окно со списком имеющихся сетевых подключений. В данном окне нужно выделить значок подключения, которое необходимо защитить брандмауэром, и в левой части окна в группе задач Сетевые задачи щелкнуть на ссылке Изменение настроек подключения (рис. 4.1).

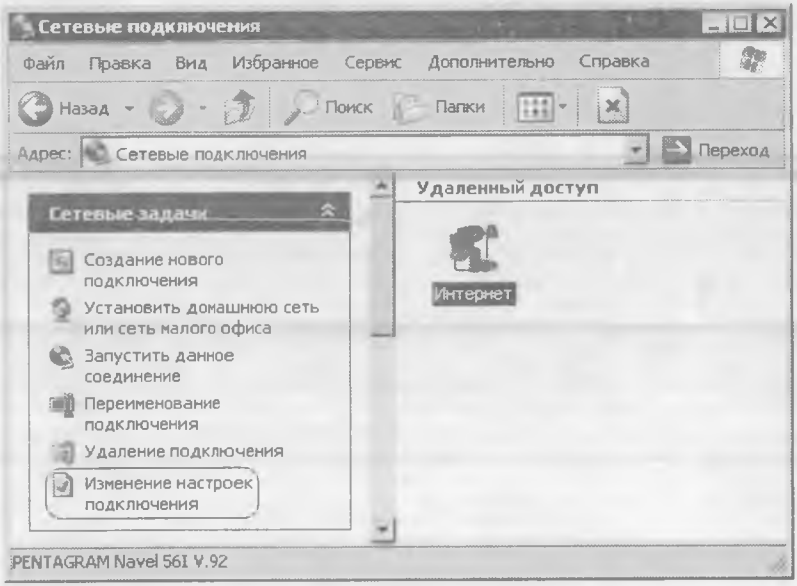

Рис. 4.1. Переход в режим изменения настроек подключения

После выполнения указанных действий на экране появится окно просмотра и редактирования свойств текущего подключения. В данном окне следует перейти на вкладку Дополнительно (рис. 4.2).

Чтобы включить брандмауэр текущего подключения, на данной вкладке следует установить флажок Защитить мое подключение к Интернету.

Кроме штатного брандмауэра Windows XP, в настоящее время на рынке представлено достаточное количество брандмауэров сторонних разработчиков. Среди них можно рекомендовать брандмауэр ZoneAlarm. Интерфейс программы представлен на рис. 4.3.

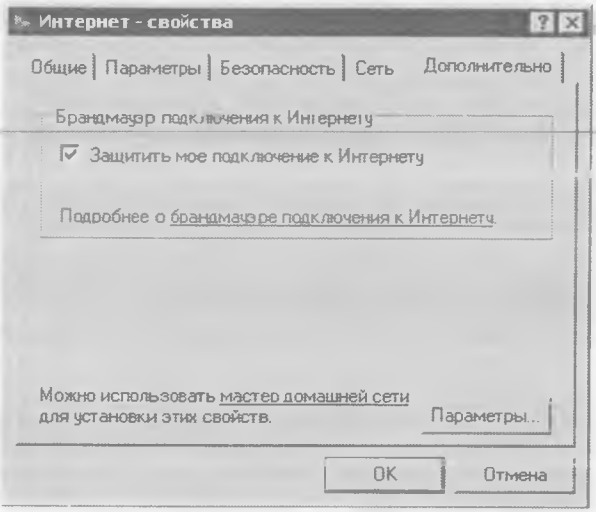

Рис. 4.2. Окно редактирования свойств, вкладка Дополнительно

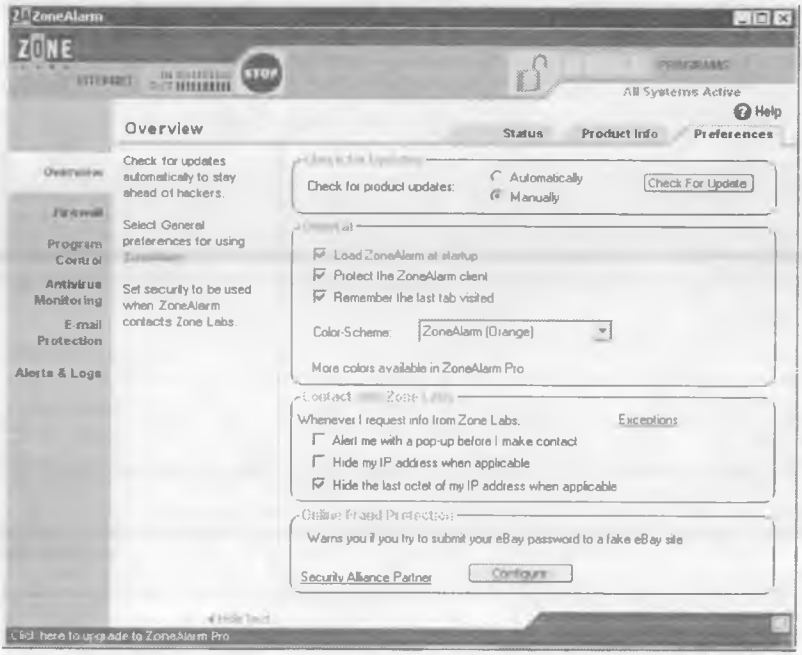

Рис. 4.3. Программа ZoneAlarm

К несомненным достоинствам программы можно отнести то, что она имеет как платную, так и бесплатную версии, причем возможностей бесплатной версии вполне достаточно для защиты домашнего компьютера. Недостаток — программа не поддерживает русский язык (по крайней мере, так было на момент написания данной книги). В брандмауэре ZoneAlarm предусмотрена возможность тонкой настройки параметров защиты. В частности, пользователь самостоятельно указывает приложения, которым разрешен выход в Интернет (чаще всего это браузер, почтовая программа, ICQ и т. п.), и определяет параметры доступа в компьютер извне (иначе говоря, полностью контролирует входящий и исходящий трафик). Кроме этого, можно поместить программу в автозагрузку, включить режим скрытия своего IP-адреса и др.

Следует отметить, что программа ZoneAlarm в настоящее время является одним из самых надежных брандмауэров.

Анонимность работы в Интернете

Многие пользователи Интернета наверняка неоднократно задавали себе вопрос: можно ли обеспечить анонимность работы в Интернете? Ведь это позволяет получить множество преимуществ. Например, можно посещать любые ресурсы, и никто не вычислит пользователя по IP-адресу. Кроме этого, можно получить доступ к веб-ресурсам, которые закрыты для обычного доступа (например, заблокированы системным администратором). Да и вообще — очевидно, что лучше не оставлять в Сети никаких следов, так как ими может воспользоваться кто угодно, в частности злоумышленники. Рассмотрим некоторые варианты обеспечения анонимности при работе в Интернете.

«Заметаем следы» на локальном компьютере

Многие наверняка сталкивались с ситуацией, когда к рабочему компьютеру имеют доступ несколько сотрудников. Можно ли после работы в Интернете сделать так, чтобы о посещенных ресурсах не узнали другие пользователи данного компьютера? Особенно это актуально, если к компьютеру имеет доступ начальство...

Рассмотрим, как можно решить эту проблему с помощью браузера Internet Explorer.

Чтобы перейти в режим удаления следов своего пребывания в Интернете, выполните команду главного меню Сервис ▸ Свойства

обозревателя и в открывшемся окне перейдите на вкладку Общие (содержимое данной вкладки показано на рис. 4.4).

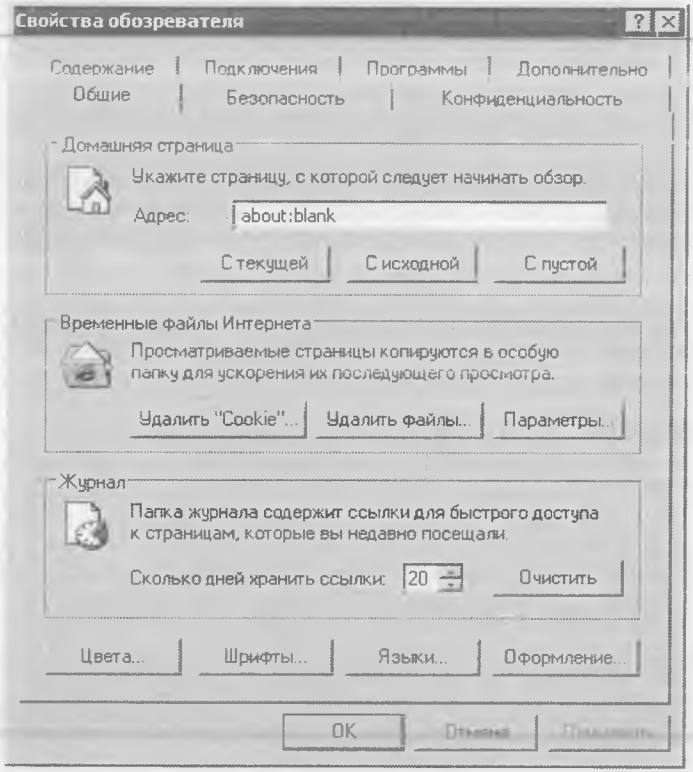

Рис. 4.4. Свойства обозревателя, вкладка Общие

На данной вкладке обратите внимание на кнопки Удалить "Cookie", Удалить файлы и Очистить. Остановимся на них подробнее.

С помощью кнопки Удалить "Cookie" можно быстро удалить с локального диска все файлы Cookie. Эти файлы, создаваемые веб-узлом, содержат информацию о пользователе, которая применяется при посещении данного узла. При нажатии кнопки Удалить "Cookie" появится дополнительный запрос на подтверждение данного действия.

Кнопка Удалить файлы предназначена для быстрого удаления всех временных файлов Интернета. По умолчанию папка с таки-

ми файлами располагается по адресу C:\Documents and Settings\Имя пользователя\Local Settings\Temporary Internet Files. Однако при необходимости этот путь можно изменить. Для этого следует нажать кнопку Параметры, открывающую одноименное окно. В данном окне нажмите кнопку Переместить, затем в появившемся окне Обзор папок по обычным правилам Windows укажите требуемый путь.

Почему желательно удалить содержимое папки с временными файлами? Дело в том, что посторонний пользователь, заглянув в эту папку, может увидеть там все, что вы видели в Интернете. Кстати, для быстрого открытия данной папки можно воспользоваться кнопкой Просмотр файлов, которая находится в окне Параметры рядом с кнопкой Переместить.

Если вы бродили по Интернету, используя только ссылки, поисковики и т. п., то основной «компромат» вы удалите описанным способом. Однако если вы набирали что-то в адресной строке Internet Explorer, то вводимые адреса сохранились в ее раскрывающемся списке.

Для очистки раскрывающегося списка адресной строки следует воспользоваться кнопкой Очистить, которая находится на вкладке Общие в окне редактирования свойств обозревателя (см. рис. 4.4). Однако необходимо учитывать, что программе все равно, какие адреса «хорошие», а какие — «плохие». При нажатии данной кнопки из адресной строки будут удалены все адреса, поэтому предварительно рекомендуется изучить данный список и сохранить нужные.

При необходимости можно восстановить содержимое списка адресной строки после того, как он был очищен. Для этого достаточно восстановить систему с помощью специально предназначенной функции (ее описание приведено ниже, в разд. 7).

Как спрятаться, находясь в Интернете

Использование прокси-сервера. Наиболее распространенный способ, позволяющий скрыть «свое истинное лицо» (а точнее, IP-адрес) при работе в Интернете, — это использование прокси-сервера.

Что же представляет собой прокси-сервер и каким образом его использовать?

Прокси-сервер — это компьютер, находящийся между компьютером пользователя и Интернетом. Иначе говоря, это своего рода посредник, промежуточное звено. Анонимность при использовании прокси-сервера достигается за счет того, что вместо реального

IP-адреса компьютера, с которого пользователь вышел в Интернет, подставляется совершенно другой IP-адрес. Это позволяет, например, посещать веб-ресурсы, зайти на которые без использования прокси-сервера невозможно. Кроме того, использование прокси-сервера часто позволяет значительно увеличить скорость работы в Интернете, хотя иногда возможен и противоположный эффект (все зависит от конкретного прокси-сервера).

Каким же образом использовать прокси-сервер? Сначала необходимо найти его адрес и номер порта. Поинтересуйтесь у знакомых: может, кто-то знает адрес и порт реально действующего прокси-сервера. Если нет — достаточно войти в Интернет, набрать в любом поисковике «прокси-сервер» или что-то в этом роде и просмотреть результаты поиска.

Следует учитывать, что поисковик, вероятнее всего, выдаст большое количество списков с адресами и номерами портов прокси-серверов, но большая часть из них нерабочие. Определить, какой прокси-сервер является рабочим, можно вручную (это долгий и нудный процесс), а можно с помощью специальных утилит, которые имеются в Интернете. Принцип использования большинства таких утилит прост: в программу загружается список портов и адресов, и через некоторое время она выдает только действующие.

Чтобы выйти в Интернет через прокси-сервер, необходимо соответствующим образом настроить браузер. Рассмотрим настройку параметров на примере обозревателя Internet Explorer.

В окне Свойства обозревателя, открываемом с помощью команды главного меню Сервис ▸ Свойства обозревателя, перейдите на вкладку Подключения (рис. 4.5).

На данной вкладке нажмите кнопку Настройка (эта кнопка выделена на рис. 4.5). В результате на экране появится окно Интернет Параметры, изображенное на рис. 4.6.

Чтобы включить режим использования прокси-сервера, в области Прокси-сервер данного окна нужно установить флажок Использовать прокси-сервер для этого подключения (не применяется для других подключений). После этого станут доступными для редактирования поля Адрес и Порт, в которые с клавиатуры введите соответственно IP-адрес используемого прокси-сервера и номер порта. Выполненные настройки действительны только для подключения, выбранного в окне свойств обозревателя на вкладке Подключения (см. рис. 4.5).

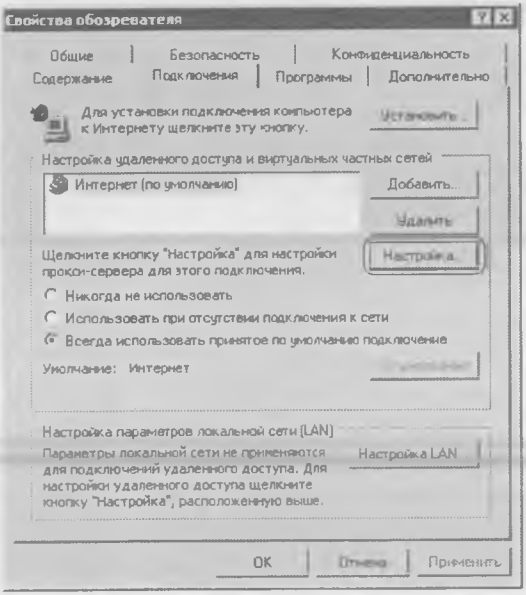

Рис. 4.5. Свойства обозревателя, вкладка Подключения

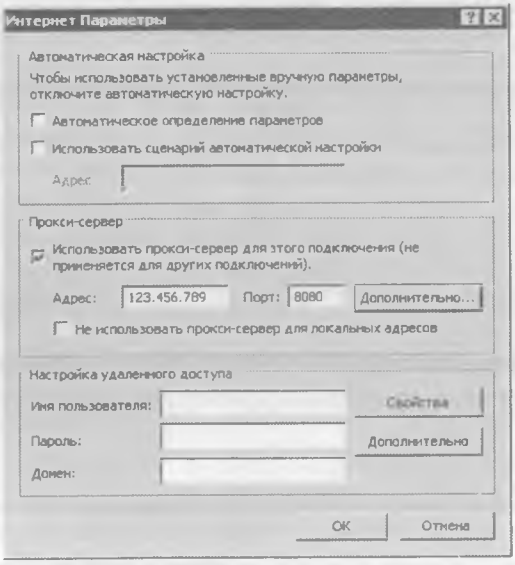

Рис. 4.6. Окно Интернет Параметры

С помощью кнопки Дополнительно, которая расположена справа от поля Порт, можно перейти в режим настройки дополнительных параметров прокси-сервера. При нажатии данной кнопки на экране появится окно, изображенное на рис. 4.7.

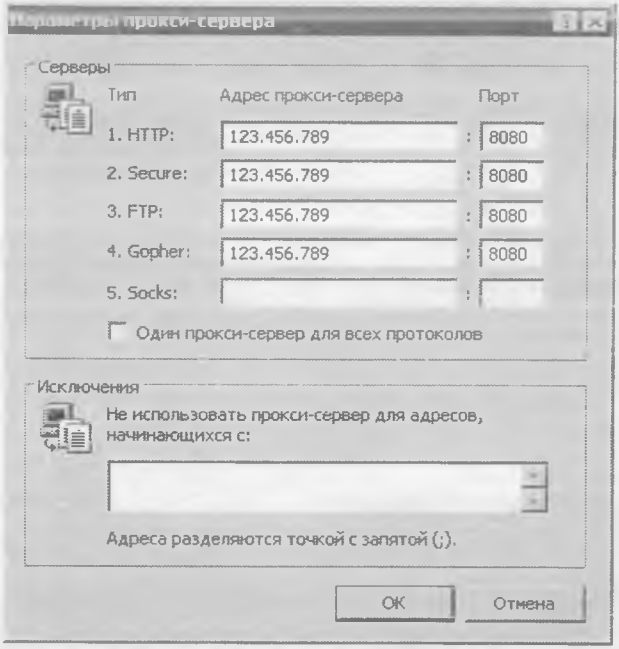

Рис. 4.7. Дополнительные параметры прокси-сервера

Данное окно содержит две области: Серверы и Исключения.

В области Серверы можно для каждого типа протокола указать отдельный прокси-сервер. Для этого нужно снять флажок Один прокси-сервер для всех протоколов и ввести в соответствующие поля IP-адреса и порты используемых прокси-серверов. По умолчанию данный флажок установлен, а для редактирования доступны только поля, соответствующие протоколу HTTP.

В выделенной области Исключения можно создать список веб-адресов, для которых прокси-сервер использоваться не будет.

Использование анонимайзера. Наряду с прокси-серверами в настоящее время широкое распространение получили анонимайзеры. Анонимайзер — это, по сути, разновидность прокси-сервера. Основ-

ное отличие состоит в том, что для использования анонимайзера не нужно выполнять никаких дополнительных настроек. Как правило, анонимайзер не имеет номера порта, а представляет собой обычную веб-страницу со стандартным интернет-адресом. Например, один из популярных русскоязычных анонимайзеров расположен по адресу http://www.anonymizer.ru.

Порядок использования анонимайзера достаточно прост и напоминает работу с обычным поисковиком. Каждый анонимайзер имеет свою адресную строку, в которую следует ввести требуемый адрес и нажать расположенную рядом кнопку (она может называться Перейти, Go и т. п. в зависимости от конкретного анонимайзера). В результате вы перейдете на соответствующую страницу (сайт). Обратите внимание на содержимое адресной строки интернет-обозревателя: хорошо знакомый адрес будет выглядеть весьма непривычно. Например, если обычно он выглядит как www.piter.com, то при использовании анонимайзера http://www.anonymizer.ru адрес примет вид: http://www.anonymizer.ru/cgi-bin/webprox?session=demo&form=header&url=www.piter.com.

В некоторых анонимайзерах можно, хотя и не обязательно, настроить некоторые параметры. Как правило, элементы управления параметрами представляют собой флажки или переключатели. С их помощью можно разрешать/запрещать отображение сценариев, рекламы, рисунков и др.

Следует отметить, что действующий анонимайзер найти гораздо проще, чем действующий прокси-сервер.

5. Локальная сеть под контролем

Многие считают, что безопасность локальной сети — это головная боль исключительно системного администратора. Однако это не совсем так. В настоящее время нередко в одной квартире имеется несколько компьютеров, объединенных в локальную сеть. Все большую популярность приобретают локальные сети, в которые объединено несколько стоящих по соседству многоквартирных домов. Случаев применения локальных сетей за пределами офиса без участия системного администратора достаточно много.

В этой главе рассмотрим вопросы удаленного администрирования компьютера, а также контроля за интернет-трафиком (это бывает полезно, например, для отслеживания возможной утечки информации).

Удаленное администрирование

Смысл удаленного администрирования заключается в том, что оно позволяет выполнять любые действия на удаленном компьютере (открывать файлы и папки, запускать приложения, изменять параметры настройки и т. д.). Кроме этого, возможности удаленного администрирования позволяют следить за тем, что происходит на удаленном компьютере (например, днем родители могут следить с рабочего компьютера, чем занимается ребенок на домашнем компьютере).

Удаленное подключение в операционной системе Windows XP

В системе Windows XP реализована возможность дистанционного подключения к удаленному компьютеру. Для этого необходимо, чтобы на обоих компьютерах (рабочем и удаленном) была установлена Windows XP и они были подключены к локальной сети или Интернету.

Для подключения к удаленному компьютеру следует выполнить команду Пуск ▸ Все программы ▸ Стандартные ▸ Связь ▸ Подключение к удаленному рабочему столу. В результате на экране появится окно, изображенное на рис. 5.1.

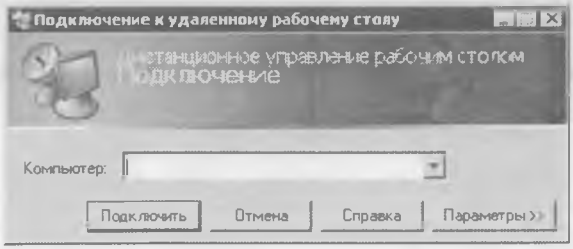

Рис. 5.1. Подключение к удаленному компьютеру

В данном окне в поле Компьютер следует ввести с клавиатуры или выбрать из раскрывающегося списка IP-адрес или имя компьютера, к которому нужно подключиться, и нажать кнопку Подключить. При необходимости можно просмотреть и отредактировать параметры подключения. Для этого следует нажать кнопку Параметры, в результате чего окно примет вид, показанный на рис. 5.2.

В зависимости от функционального назначения параметры подключения сгруппированы на следующих вкладках: Общие, Экран, Локальные ресурсы, Программы и Дополнительно. Кратко остановимся на каждой из них.

На вкладке Общие (она открыта на рис. 5.2) настраивают общие параметры подключения: имя или IP-адрес удаленного компьютера, имя рабочей группы или домена (если требуется) и пароль (при необходимости). Кроме того, на этой вкладке можно сохранить текущие параметры подключения в отдельном файле для последующего использования. Для этого нажмите кнопку Сохранить как и в открывшемся окне по обычным правилам Windows укажите имя файла и путь для сохранения. Чтобы впоследствии использовать сохраненные настройки, достаточно нажать кнопку Открыть и в появившемся окне указать путь к требуемому файлу.

На вкладке Экран настраивают некоторые параметры экрана. В частности, с помощью соответствующего ползунка указывают размер экрана удаленного компьютера (можно установить полноэкранный режим), а также требуемую цветовую палитру.

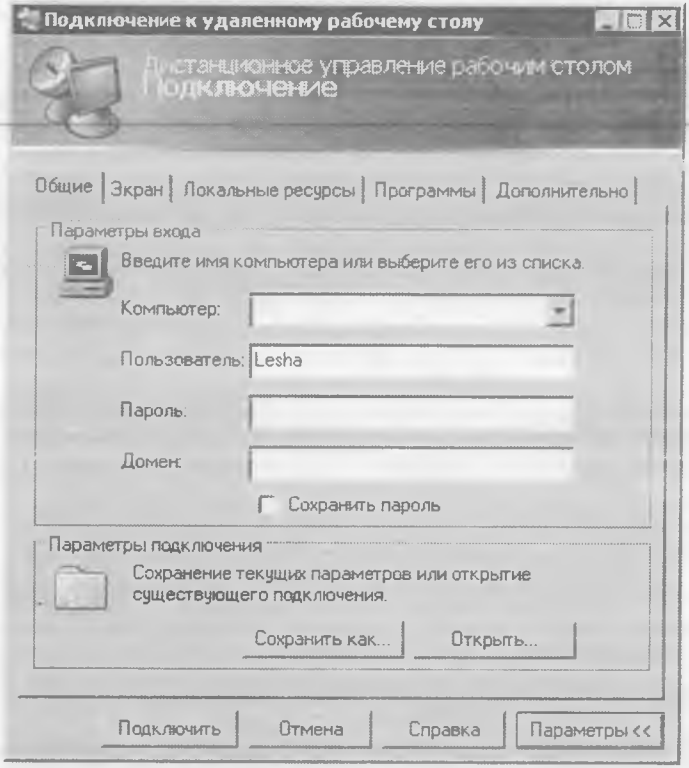

Рис. 5.2. Просмотр и редактирование параметров подключения

Параметры, расположенные на вкладке Локальные ресурсы, предназначены для настройки звукового оформления событий, использования сочетаний клавиш, а также определения устройств, к которым следует автоматически подключаться при соединении с удаленным компьютером.

При необходимости можно сделать так, что при подключении к удаленному компьютеру будет автоматически запускаться какая-либо программа. Для этого на вкладке Программы установите флажок При подключении запускать следующую программу, после чего в соответствующее поле ввести путь к требуемому файлу.

На вкладке Дополнительно настраивают дополнительные параметры выбранного в данный момент подключения. В частности, устанавливают требуемую скорость соединения, а также при необходи-

мости включают использование на удаленном компьютере фонового рисунка Рабочего стола, визуальных эффектов и др.

Следует отметить, что возможность удаленного подключения к компьютеру, реализованная в Windows XP, предназначена не столько для удаленного администрирования, сколько для удаленной работы на компьютере. Например, подключившись дома к рабочему компьютеру, можно завершить то, что не удалось сделать в течение рабочего дня. Для удаленного администрирования целесообразно использовать специально разработанные программы, например Remote Administrator.

Программа Remote Administrator

Программа Remote Administrator в настоящее время является одной из самых популярных программ, предназначенных для удаленного администрирования. Эта программа условно бесплатная: ее можно использовать в течение 30 дней, после чего необходимо приобрести лицензию или удалить Remote Administrator с компьютера. Достоинством программы является то, что она поддерживает русский язык. Remote Administrator можно скачать по адресу: www.radmin.com/ru/download. Размер архива, предлагаемого к скачиванию, составляет чуть менее 2 Мбайт. Программа работает со всеми операционными системами семейства Windows начиная с Windows 95.

Remote Administrator состоит из двух основных составных частей: Radmin Server и Radmin Viewer.

Radmin Server устанавливают на удаленном компьютере. Следует учитывать, что в операционных системах Windows NT/2000/XP/2003 для этого необходимо обладать правами администратора, поскольку в процессе установки создается новая системная служба. Radmin Server передает изображение с экрана удаленного компьютера на локальный.

Radmin Viewer устанавливают на рабочем компьютере. Эта часть программы отображает на экране локального компьютера содержимое экрана удаленного компьютера. С помощью Radmin Viewer можно работать с удаленным компьютером: следить за ним, управлять, администрировать и т. д.

Для успешной работы необходимо, чтобы компьютеры были соединены между собой по протоколу TCP/IP.

После установки на удаленном компьютере Radmin Server рекомендуется просмотреть и при необходимости отредактировать

настройки данной программы. Чтобы перейти в соответствующий режим, следует выполнить команду Пуск ▸ Все программы ▸ Remote Administrator ▸ Настройка Remote Administrator server. В результате на экране появится окно, изображенное на рис. 5.3.

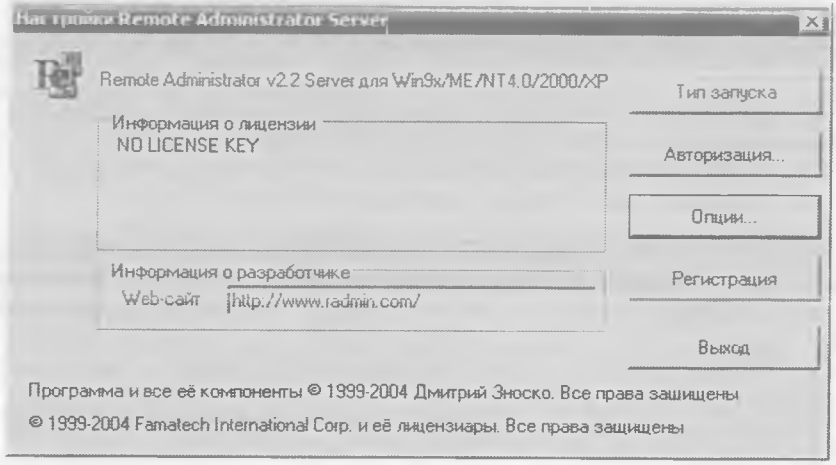

Рис. 5.3. Настройка Remote Administrator Server

Для настройки основных параметров следует нажать кнопки Тип запуска и Опции.

При нажатии кнопки Тип запуска на экране появится окно, представленное на рис. 5.4.

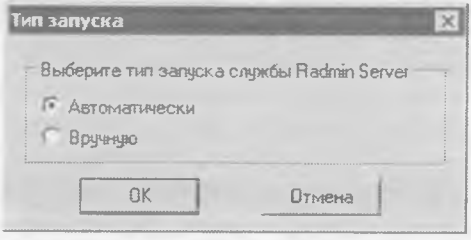

Рис. 5.4. Выбор типа запуска Radmin Server

В данном окне с помощью соответствующего переключателя устанавливают требуемый тип запуска Radmin Server. По умолчанию переключатель установлен в положение Автоматически, и в большин-

стве случаев изменять данную настройку не стоит. При выборе этого значения Radmin Server будет загружаться автоматически до входа пользователя в систему. Если же установить переключатель в положение Вручную, то для включения Radmin Server нужно будет запускать исполняемый файл (или непосредственно, или с помощью соответствующей команды меню Пуск).

При нажатии кнопки Опции на экране появится окно, показанное на рис. 5.5.

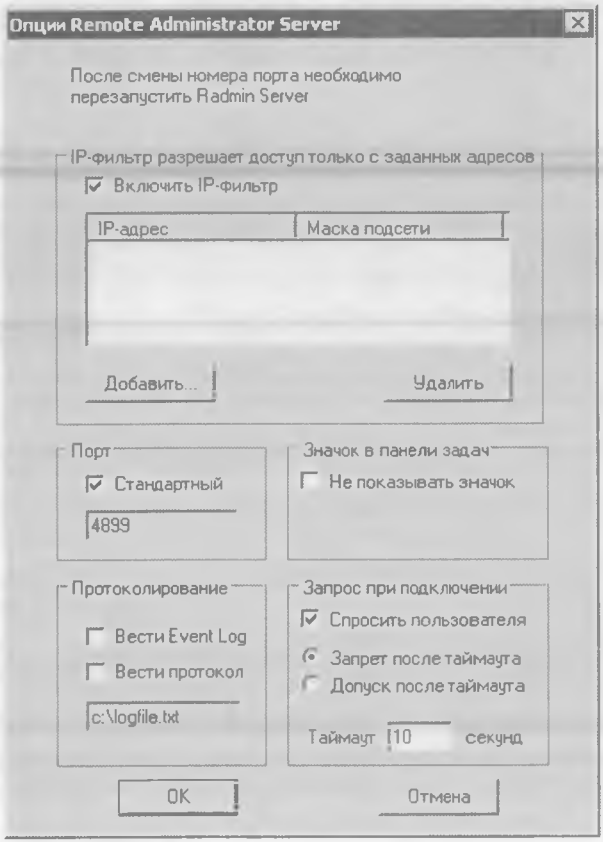

Рис. 5.5. Настройка параметров Radmin Server

В данном окне настраивают множество основных параметров, во многом определяющих работу Radmin Server.

В верхней части окна при необходимости можно установить фильтр по IP-адресам. Это означает, что подключаться к данному компьютеру смогут только компьютеры с определенными IP-адресами. Для включения фильтра нужно установить флажок Включить IP-фильтр. Чтобы добавить в список новую позицию, нажмите кнопку Добавить (работа со списком возможна только при установленном флажке Включить IP-фильтр). При нажатии данной кнопки откроется окно Добавить адрес в IP-фильтр, в котором выполняют необходимые действия. Чтобы удалить из списка ненужную позицию, следует выделить ее и нажать кнопку Удалить.

В области Порт при необходимости можно изменить номер порта. По умолчанию порту присвоен стандартный номер 4899. Чтобы его изменить, нужно снять флажок Стандартный, установленный по умолчанию. В результате станет доступным расположенное ниже поле, в которое следует с клавиатуры ввести требуемый номер порта.

Область Значок в панели задач содержит флажок Не показывать значок. Если он установлен, то значок Radmin Server не будет отображаться на Панели задач. По умолчанию этот флажок снят.

При необходимости можно вести протокол всех действий программы. Причем реализована возможность не только создания файла протокола, но и внесения информации в журнал событий (для Windows NT4.0/2000/XP/2003). Для создания файла протокола нужно установить флажок Вести протокол и в расположенное ниже поле ввести путь к файлу протокола (по умолчанию предложен путь C:\logfile.txt). Чтобы информация автоматически вносилась в журнал событий, следует установить флажок Вести Event Log. По умолчанию оба флажка сняты.

Параметры, расположенные в области Запрос при подключении, предназначены для настройки запроса, который будет появляться при подключении к удаленному компьютеру. При установленном флажке Спросить пользователя подключение будет возможно только после того как пользователь положительно ответит на соответствующий запрос. Если пользователь не ответил на запрос (например, потому что его нет за компьютером), то возможность подключения определяется положением переключателя. Если переключатель установлен в положение Запрет после таймаута, то по истечении установленного промежутка времени подключение будет разорвано. Если выбрано положение Допуск после таймаута, то

по истечении заданного интервала времени подключение к удаленному компьютеру будет установлено. Промежуток времени определяют в поле Таймаут... секунд (по умолчанию задано значение 10).

После настройки Radmin Server удаленный компьютер готов к подключению извне (напомню, что компьютеры должны быть соединены по протоколу TCP/IP).

Запустите на локальном компьютере Radmin Viewer. Рабочее окно программы представлено на рис. 5.6.

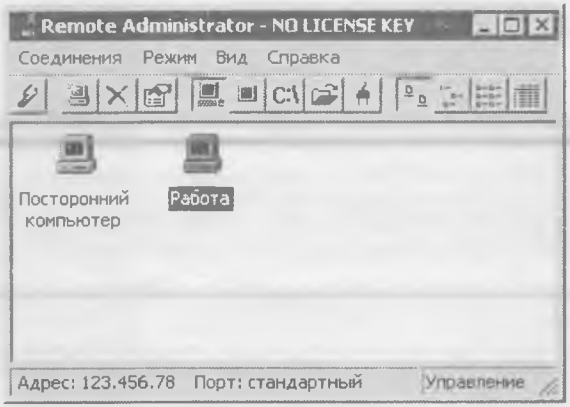

Рис. 5.6. Окно Radmin Viewer

Данное окно содержит значки созданных подключений (например, к компьютеру знакомого, к рабочему компьютеру и т. д.). При первом запуске, разумеется, в окне не будет ни одного подключения.

Чтобы создать новое подключение, нужно выполнить команду главного меню Соединения ▸ Новое или нажать клавишу Insert. При этом на экране появится окно, изображенное на рис. 5.7.

В поле Название записи данного окна с клавиатуры вводят произвольное название создаваемого подключения, а в поле IP-адрес или DNS-имя — IP-адрес или имя удаленного компьютера. Кроме этого, в соответствующем поле указывают номер порта. По умолчанию установлен стандартный порт с номером 4899, однако при необходимости это значение можно изменить. Для этого нужно снять флажок Стандартный порт.

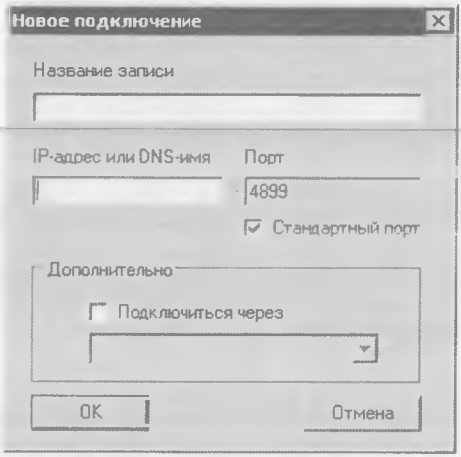

Рис. 5.7. Создание нового подключения

В области Дополнительно находится флажок Подключиться через. При установленном данном флажке становится доступным поле, в которое вводят имя компьютера, через который нужно подключиться к удаленному компьютеру (своего рода «прокси-сервер»). Это значение вводят с клавиатуры или выбирают из раскрывающегося списка, обычно содержащего существующие подключения. Данная возможность полезна, если нет прямого соединения по протоколу TCP/IP с удаленным компьютером, но такое соединение есть с промежуточным компьютером, а у него, в свою очередь, с удаленным. Замечу, что промежуточный компьютер может понадобиться для соединения с удаленным и в других ситуациях. При этом следует учитывать, что Radmin Server следует установить и на промежуточном, и на удаленном компьютерах.

Чтобы завершить процесс создания нового подключения, нажмите кнопку OK. С помощью кнопки Отмена можно выйти из данного режима без сохранения изменений.

Для соединения с удаленным компьютером выделите требуемое подключение и выполните команду главного меню Соединения ▸ Подключиться (или нажмите клавишу Enter). Для этого можно также воспользоваться командой Соединения ▸ Подключиться к. В данном режиме создается новое подключение, которое можно сразу же запустить. При этом с помощью соответствующего переключателя выберите требуемый режим соединения.

Для выбора режима соединения предназначены также следующие команды меню Режим.

- Управление — управление удаленным компьютером с помощью мыши и клавиатуры локального компьютера. При этом на мониторе отображается экран удаленного компьютера.
- Просмотр — слежение за удаленным компьютером (просмотр содержимого экрана).
- Телнет — режим, применимый только к компьютерам, работающим под управлением операционных систем Windows NT/2000/XP/2003.
- Обмен файлами — обмен с удаленным компьютером файлами и папками. Возможности программы предусматривают обмен файлами, объем которых не превышает 2 Гбайт, и папками, содержащими не более 20 000 объектов.
- Выключение — перезагрузка, выключение, приостановка работы и завершение сеанса работы для пользователя, в данный момент работающего на удаленном компьютере.

При необходимости можно изменить параметры существующего подключения. Для перехода в соответствующий режим требуется выделить нужное подключение и выполнить команду главного меню Соединения ▸ Свойства или аналогичную команду контекстного меню. Для удаления подключения предназначена команда Соединения ▸ Удалить.

Очевидно, что с помощью программы Remote Administrator можно не только в режиме реального времени следить за тем, что происходит на удаленном компьютере, но также вмешиваться в работу удаленного пользователя и выполнять другие действия по управлению и администрированию. При этом возможности программы позволяют контролировать не только один, но и несколько удаленных компьютеров, отслеживая все, что происходит в локальной сети.

Утечка информации и контроль интернет-трафика

Вопрос возможной утечки информации волнует многих пользователей. Это неудивительно: в настоящее время данная проблема достаточно актуальна. Как упоминалось, для похищения чужой информации существует множество шпионских программ. Кроме того,

причиной проблемы может быть и человеческий фактор: не исключено, что один из участников локальной сети с корыстной целью тайком передает какую-либо секретную информацию через Интернет.

В этой главе рассказано о том, каким образом можно предотвратить утечку информации из локальной сети через Интернет.

Конечно, можно решить эту проблему кардинально, запретив выход в Интернет с компьютеров всех участников локальной сети. Однако очевидно, что в большинстве случаев это совершенно неприемлемо. Поэтому целесообразно использовать специальные программы, предназначенные для контроля интернет-трафика. Рассмотрим две такие популярные программы.

Time&Mb

Программа Time&Mb представляет собой небольшую утилиту, предназначенную для контроля интернет-трафика на локальном компьютере. Программа поддерживает русский язык. Размер архива, предлагаемого для скачивания, составляет около 200 Кбайт. Программу Time&Mb можно скачать по адресу www.bikart.narod.ru.

Time&Mb не требует установки. Распакованный архив представляет собой исполняемый файл TimeMB.exe, предназначенный для запуска утилиты.

Интерфейс программы показан на рис. 5.8.

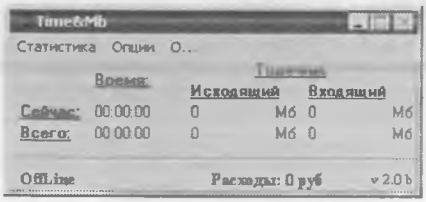

Рис. 5.8. Программа Time&Mb

На рисунке видно, что программа демонстрирует размер исходящего и входящего трафика, а также денежные затраты на работу в Интернете. Чтобы программа могла рассчитать сумму расходов, необходимо соответствующим образом настроить параметры. Для перехода в режим настройки следует воспользоваться командой главного меню Опции ▸ Стоимость ▸ Время. В результате на экране появится окно, изображенное на рис. 5.9.

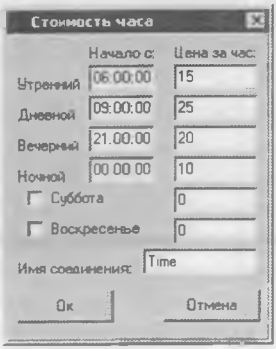

Рис. 5.9. Настройка расчета затрат

В данном окне указывают стоимость одного часа работы в Интернете утром, днем, вечером и ночью, а также в субботу и воскресенье. На основании этой информации программа рассчитывает денежные затраты и показывает эту сумму в информационной строке Расходы главного окна.

Аналогичным образом можно настроить расчет суммы расходов в зависимости от трафика. Для перехода в режим настройки следует выполнить команду главного меню Опции ▸ Стоимость ▸ Трафик.

С помощью команды главного меню Статистика можно перейти в режим просмотра статистики работы в Интернете на любую указанную дату. После выполнения этой команды откроется окно, которое показано на рис. 5.10.

Рис. 5.10. Окно просмотра статистики

В данном окне можно указать день, для которого необходимо просмотреть статистику работы в Интернете. Если требуется просмотреть статистику за какой-то месяц, то необходимо выбрать его из раскрывающегося списка За месяц и нажать кнопку Показать. В результате на экране появится окно, содержащее общее время работы в Интернете, размер входящего и исходящего трафика в мегабайтах, а также сумму денежных затрат на работу в Интернете.

Программа Time&Mb достаточно небольшая, она предназначена в основном для контроля интернет-трафика на локальном компьютере (это целесообразно, например, когда за одним компьютером по очереди работают разные пользователи). Однако существуют более масштабные программы, не только позволяющие контролировать интернет-трафик, но и обладающие многими другими возможностями. Такие программы обычно используются в домашних, местных и офисных локальных сетях. Одна из подобных программ рассмотрена в следующем подразделе.

Lan2Net

Программа Lan2Net предназначена для подсчета интернет-трафика, а также для ограничения доступа как в локальную сеть, так и в Интернет. Данная программа поддерживает русскоязычный интерфейс. Она является условно бесплатной: демонстрационную версию можно использовать в течение 30 суток. Размер установочного файла, предлагаемого к скачиванию, примерно равен 2,3 Мбайт. Программу можно скачать по адресу: www.lan2net.ru/l2n_download.shtml.

Функциональные возможности Lan2Net позволяют решать следующие задачи:

- подключение локальной сети к Интернету;
- подсчет интернет-трафика как отдельных пользователей, так и групп пользователей;
- тонкое распределение ресурсов пропускного канала между пользователями;
- ограничение доступа к тем или иным ресурсам;
- преобразование IP-адресов в URL;
- защита локальной сети от внешних атак и проникновения вредоносных приложений (функции брандмауэра).

Программа Lan2Net состоит их трех основных частей:

- межсетевой экран — предназначен для подсчета интернет-трафика;
- интерфейс администратора — для управления работой пользователей, настройки некоторых параметров и др.;
- клиент пользователя — для просмотра интернет-трафика, выбранного пользователем.

В этой книге подробно рассмотрим интерфейс администратора, поскольку он является основным инструментом программы.

После завершения установки программы необходимо перезагрузить компьютер, о чем вы узнаете из соответствующего информационного окна. После перезагрузки на экране появится окно Мастера конфигурации, с помощью которого выполняют предварительную настройку параметров работы. Мастер автоматически появляется только один раз: после установки программы и перезагрузки компьютера. Однако впоследствии его можно вызвать командой главного меню Мастер настройки ▸ Запуск мастера.

При вызове Мастера конфигурации из интерфейса администратора будут удалены все настройки. Кроме того, станет недоступной статистика прошлых периодов.

Интерфейс администратора программы Lan2Net изображен на рис. 5.11.

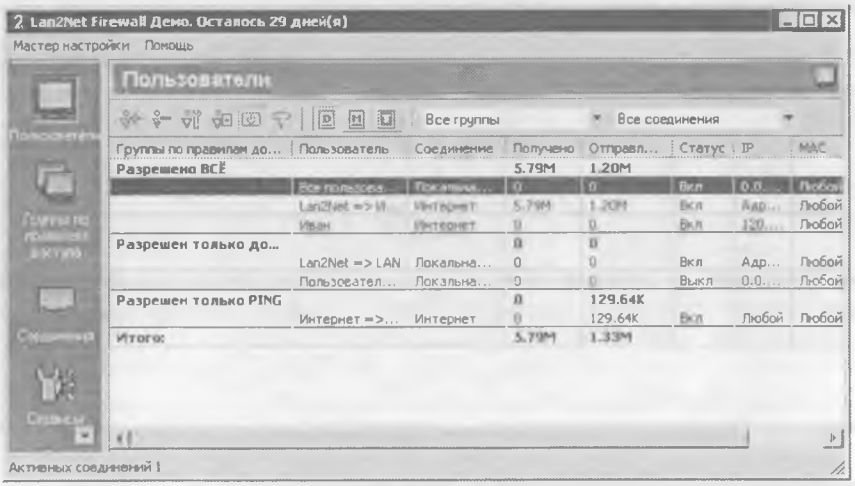

Рис. 5.11. Интерфейс администратора

Данное окно содержит несколько разделов, каждый из которых предназначен для определенного режима работы. Перейти в нужный раздел можно с помощью соответствующих кнопок, расположенных в левой части окна.

Пользователи. Раздел Пользователи (он открыт на рис. 5.11) содержит список пользователей и групп пользователей, входящих в состав локальной сети. Для каждого пользователя или группы пользователей в соответствующих столбцах отображается характерная информация (имя пользователя, его статус, IP-адрес и др.). Кроме этого, показаны размеры входящего и исходящего трафика (столбцы Получено и Отправлено). При этом может отображаться трафик за день, за месяц и общий (требуемый режим устанавливают с помощью соответствующих кнопок панели инструментов).

Для просмотра подробной статистики по определенному пользователю нужно выделить его в списке и в контекстном меню выбрать пункт Статистика. Можно также нажать соответствующую кнопку на панели инструментов. В результате на экране появится окно, показанное на рис. 5.12.

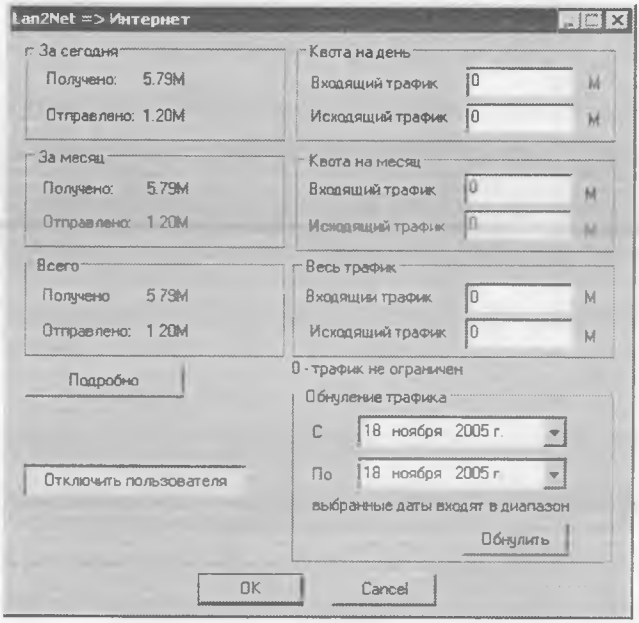

Рис. 5.12. Статистика пользователя

В данном окне для выбранного пользователя показывается размер входящего и исходящего трафика за текущий день, месяц и всего. В правой части окна отображается лимит (квота) исходящего и входящего трафика для данного пользователя на день, месяц и всего. Очевидно, что с помощью такого механизма очень удобно контролировать входящий и исходящий интернет-трафик для каждого пользователя. В этом же окне можно с помощью соответствующей кнопки подключать или отключать пользователя от Интернета.

Для добавления в список новой позиции нужно, находясь в списке пользователей, щелкнуть правой кнопкой мыши и выполнить команду контекстного меню Добавить. Кроме этого, можно воспользоваться соответствующей кнопкой панели инструментов. В результате выполнения любого из этих действий на экране появится окно, изображенное на рис. 5.13.

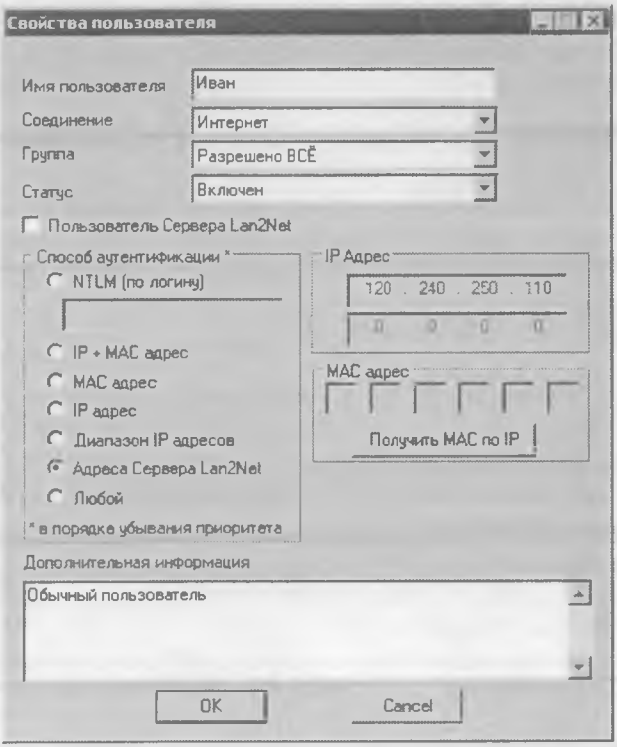

Рис. 5.13. Добавление пользователя

В данном окне с помощью соответствующих параметров определяют свойства добавляемого пользователя. В поле Имя пользователя с клавиатуры вводят произвольное имя. Значения полей Соединение, Группа и Статус выбирают из соответствующих раскрывающихся списков. В поле Соединение указывают имя сетевого соединения, для которого будет подсчитываться трафик. Поле Группа предназначено для выбора имени группы, к которой необходимо отнести данного пользователя. В поле Статус указывают статус пользователя (разрешено ли ему выходить во внешнюю сеть). Статус пользователя впоследствии можно изменить как вручную, например в режиме редактирования свойств пользователя или в режиме просмотра статистики, так и автоматически, после превышения лимита выделенного интернет-трафика (при этом учитывается как индивидуальный лимит пользователя, так и лимит, выделенный группе).

В средней части окна выбирают требуемый способ аутентификации пользователя. Переключатель Способ аутентификации доступен только при снятом флажке Пользователь Сервера Lan2Net (за исключением положений NTLM по логину и Адреса Сервера Lan2Net).

В нижней части окна в поле Дополнительная информация при необходимости можно ввести с клавиатуры дополнительную информацию произвольного характера, относящуюся к данному пользователю.

Чтобы изменить перечисленные параметры, достаточно выделить пользователя в списке и выполнить команду контекстного меню Свойства. При этом на экране откроется то же окно, что и при добавлении пользователя (см. рис. 5.13).

Для удаления пользователя из списка нужно выделить соответствующую позицию и выполнить команду контекстного меню Удалить.

Группы по правилам доступа. В данном разделе определяют правила доступа в Интернет для каждой группы пользователей. Содержимое этого раздела показано на рис. 5.14.

В верхней части окна из раскрывающегося списка выбирают имя группы, для которой необходимо настроить правила доступа. При необходимости в список можно добавить новую группу, а также удалить имеющуюся. Для этого предназначены соответствующие кнопки, расположенные справа от списка.

Удалить группу из списка можно только после уничтожения всех созданных для нее правил на вкладке Правила доступа. После удаления каждого правила необходимо нажимать кнопку Применить, расположенную в правом нижнем углу окна.

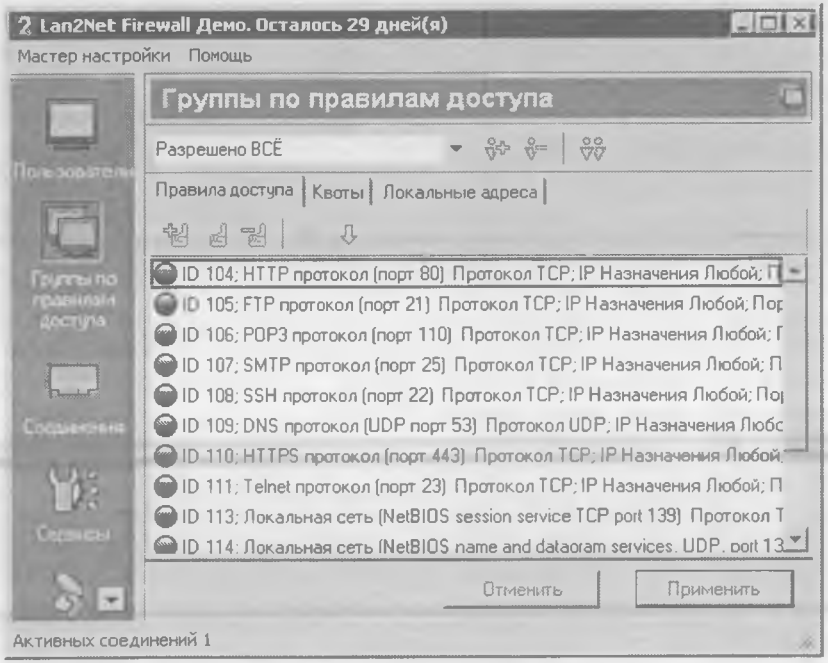

Рис. 5.14. Раздел Группы по правилам доступа

Окно данного раздела содержит три вкладки: Правила доступа, Квоты и Локальные адреса. Кратко остановимся на каждой из них.

На вкладке Правила доступа перечислены правила, которые установлены для группы, выбранной из раскрывающегося списка вверху окна. Следует учитывать, что эти правила выполняются в строгой последовательности (сверху вниз). Для изменения порядка следования правил в списке предназначены кнопки со стрелками, расположенные в правой части панели инструментов (см. рис. 5.14). Для добавления в список нового правила нужно воспользоваться командой контекстного меню Добавить или соответствующей кнопкой панели инструментов. При выборе пункта Добавить контекстного меню на экране появится окно редактирования свойств правила, в котором выполняют необходимые действия по созданию нового правила (присваивают название, выбирают протокол, указывают IP-адрес и др.). Если же для добавления правила использовать соответствующую кнопку панели инструментов, то открывается окно, в котором

следует выбрать правило из имеющихся в системе или создать свое. В последнем случае на экране также появится окно редактирования свойств правила.

Для удаления правила из списка следует выделить его и выбрать в контекстном меню пункт Удалить (можно также воспользоваться соответствующей кнопкой панели инструментов).

На вкладке Квоты лимитируют интернет-трафик для выбранной группы. В соответствующих полях указывают размер входящего и исходящего трафика на день, на месяц и всего. При необходимости можно задать лимит трафика для каждого пользователя в отдельности. Для этого следует нажать кнопку Задать квоты для пользователей группы и в открывшемся окне указать дневной, месячный и общий лимиты входящего и исходящего трафика.

На вкладке Локальные адреса можно настроить режим, при котором трафик не будет учитываться, если IP-адреса источника и назначения находятся в указанном диапазоне. Для этого в поле Диапазон От... До... нужно указать начальное и конечное значения IP-адресов и нажать кнопку Добавить. Возможности программы предусматривают использование нескольких таких диапазонов для любой группы пользователей.

Чтобы изменения, выполненные в разделе Группы по правилам доступа, вступили в силу, необходимо нажать кнопку Применить, расположенную в правом нижнем углу окна. С помощью кнопки Отменить можно отменить все изменения.

Соединения. В разделе Соединения настраивают используемые соединения (с Интернетом, локальной сетью и др.).

В верхней части окна раздела находится раскрывающийся список имеющихся соединений. Вы можете настроить то соединение, которое выбрано в данном списке. При необходимости в список можно добавить новое соединение: для этого предназначена соответствующая кнопка, расположенная справа от списка (там же находится кнопка для удаления выбранного в списке соединения). При этом нужно с клавиатуры ввести название нового соединения, настроить его параметры, после чего нажать кнопку Применить, расположенную в правом нижнем углу окна.

Чтобы внесенные изменения вступили в силу, следует нажать кнопку Применить. Для отмены изменений предназначена кнопка Отменить.

Возможности программы позволяют создавать и настраивать неограниченное количество соединений. Наиболее часто используются соединения с Интернетом и с локальной сетью.

Прочие разделы программы. Мы рассмотрели разделы программы, используемые для контроля интернет-трафика. Теперь кратко остановимся на остальных разделах программы Lan2Net.

В разделе Сервисы ведется список используемых сервисов (определенных сетевых ресурсов, например веб-серверов или подчиненных сетей). В окне редактирования для каждого сервиса указывают название, протокол, IP-адрес источника и назначения, а также порты источника и назначения. Для каждого имеющегося соединения список сервисов формируется отдельно.

В разделе Управление загрузкой канала настраивают загрузку канала для каждого соединения. Иначе говоря, здесь определяют порядок регулирования (распределения, ограничения) трафика для выбранного соединения.

Раздел Мониторинг предназначен для детального анализа каждого активного в настоящее время соединения.

В разделе Журнал можно просмотреть подробный отчет о работе каждого пользователя: в какое время и на что был потрачен конкретный входящий и исходящий трафик (при этом указывают тип соединения, IP-адреса источника и назначения и др.).

Раздел Параметры предназначен для настройки некоторых параметров работы программы (путь к лог-файлам, включение/выключение преобразования IP-адресов в URL и др.).

6. Шифрование данных

Для защиты информации от постороннего доступа целесообразно применять шифрование данных. В этой главе рассмотрим, как быстро и без особых усилий зашифровать необходимые данные: файлы, папки, электронную корреспонденцию и т. д.

Защита файлов и папок

Нововведением операционной системы Windows XP Professional является возможность автоматического шифрования файлов и папок. Отмечу, что эта функция отсутствует в Windows XP Home Edition. Кроме того, вы можете зашифровать данные только при использовании файловой системы NTFS; в системе FAT32 эта возможность недоступна.

Что же необходимо сделать, чтобы защитить важные данные с помощью шифрования? Оказывается, в Windows XP Professional это сделать совсем несложно.

На Рабочем столе или в окне Проводника щелкните правой кнопкой мыши на значке объекта (файла или папки), который необходимо зашифровать. В появившемся контекстном меню выберите пункт Свойства. В результате на экране появится окно свойств выбранного объекта. В данном окне перейдите на вкладку Общие и нажмите кнопку Другие. Откроется окно Дополнительные атрибуты (рис. 6.1).

В данном окне установите флажок Шифровать содержимое для защиты данных. Учтите, что установка данного флажка возможна только при снятом флажке Сжимать содержимое для экономии места на диске (и наоборот, сжатие содержимого возможно только при снятом флажке Шифровать содержимое для защиты данных).

Нажмите кнопку ОК, затем в окне свойств объекта нажмите кнопку Применить. После этого на экране появится окно, изображенное на рис. 6.2.

В данном окне предлагается зашифровать не только выбранный объект, но и папку, в которой он находится. При утвердительном ответе будут кодированы все объекты этой папки. Можно включить

режим, при котором впоследствии будет шифроваться только выбранный объект — для этого достаточно установить флажок Всегда шифровать только файл.

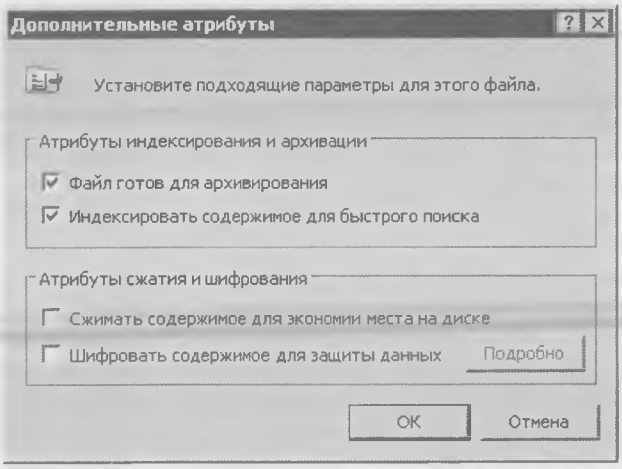

Рис. 6.1. Окно Дополнительные атрибуты

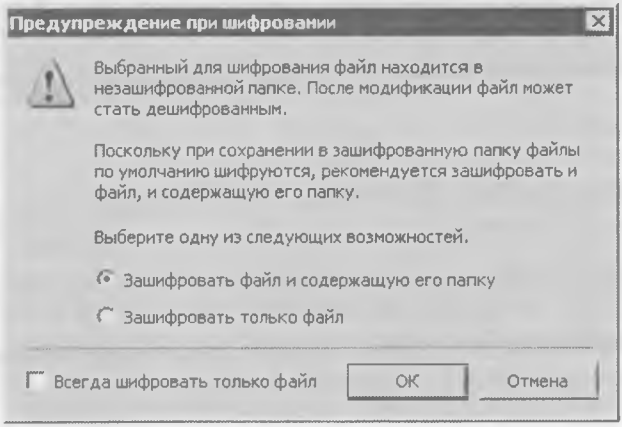

Рис. 6.2. Предупреждение при шифровании

Все объекты (файлы, папки и др.), которые в дальнейшем будут помещаться в зашифрованную папку, будут шифроваться автоматически.

Какие же преимущества дает шифрование файлов и папок, и нет ли опасности, что вы потеряете доступ к собственным кодированным данным?

Выполнять любые действия с зашифрованными объектами (просмотр, редактирование и др.) может только пользователь, который их кодировал. Таким образом, для вас эти объекты будут выглядеть как обычно, без каких-либо внешних изменений. Однако для любых других пользователей они станут полностью недоступными. Необходимо соблюдать единственное условие: никто не должен входить в систему под вашей учетной записью. Иначе говоря, прежде чем приступить к шифрованию, позаботьтесь о конфиденциальности своих учетных данных.

Вместе с этим необходимо учитывать еще одну особенность. Если вы, зашифровав данные, измените параметры своей учетной записи (имя пользователя или пароль), то можете потерять доступ к этим данным: система может «не понять» изменений. Поэтому если вы планируете изменить свои учетные данные, то кодировать необходимую информацию следует только после этого.

Если получилось так, что объекты уже зашифрованы, а вам нужно изменить учетные данные, то следует расшифровать информацию под старой учетной записью и вновь кодировать ее под новой учетной записью.

Для расшифровки данных в окне Дополнительные атрибуты, которое изображено на рис. 6.1, следует снять флажок Шифровать содержимое для защиты данных.

Шифрование электронной почты

С каждым днем увеличивается количество важной и конфиденциальной информации, которую многочисленные пользователи Интернета пересылают с помощью электронной почты. Разумеется, подобная информация всегда интересовала мошенников. Наиболее популярные на данный момент почтовые программы обладают встроенным механизмом шифрования электронной корреспонденции. Рассмотрим, каким образом шифруют электронную почту популярные программы Outlook Express и The Bat!.

В программе Outlook Express для перехода в режим шифрования следует выполнить команду главного меню Сервис ▸ Параметры и в открывшемся окне перейти на вкладку Безопасность (рис. 6.3).

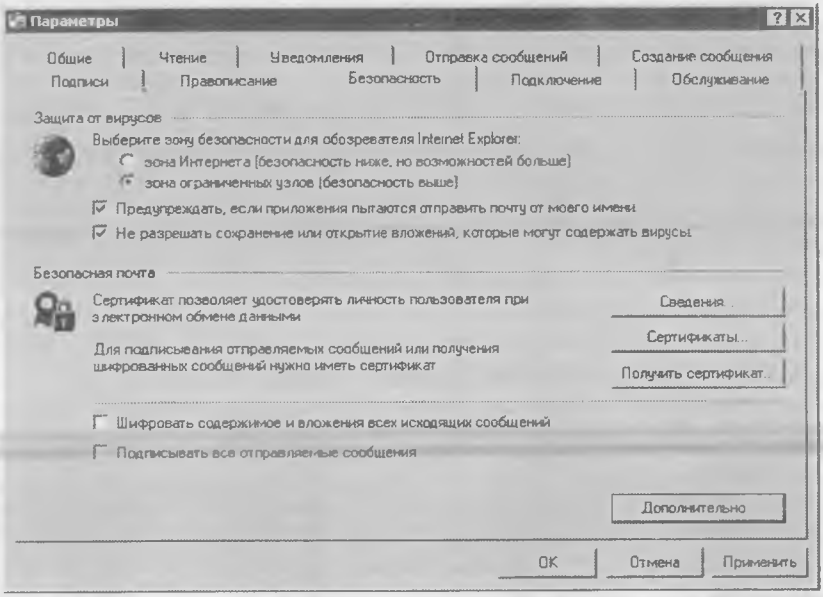

Рис. 6.3. Окно настройки параметров, вкладка Безопасность

Чтобы включить режим шифрования отправляемой электронной корреспонденции, на данной вкладке необходимо установить флажок Шифровать содержимое и вложения всех исходящих сообщений. При этом программа будет кодировать не только тексты электронных писем, но и прикрепленные к ним вложения.

Чтобы отправить кому-либо шифрованное сообщение, необходимо, чтобы в адресной книге присутствовало цифровое удостоверение получателя. В противном случае при попытке отправить кодированное сообщение на экране появится окно, в котором будет предложено отправить сообщение незашифрованным или отменить отправку.

Для перехода в режим настройки дополнительных параметров шифрования следует воспользоваться кнопкой Дополнительно вкладки Безопасность. При нажатии данной кнопки на экране появится окно Дополнительные параметры безопасности. В данном окне определяют стойкость шифрования (в битах). Если стойкость какого-либо сообщения будет меньше заданной, то на экране появится соответствующее предупреждение. При установленном флажке Шифровать

при отправке шифрованной почты самому себе программа будет автоматически отправлять шифрованную копию сообщения на ваш почтовый ящик.

В программе The Bat! также реализована возможность шифрования электронной корреспонденции, причем для каждого почтового ящика режим кодирования включается отдельно. Выполните команду главного меню Ящик ▸ Свойства почтового ящика или нажмите сочетание клавиш Shift+Ctrl+P. При этом откроется окно свойств почтового ящика. В левой части данного окна выделите пункт Параметры (рис. 6.4).

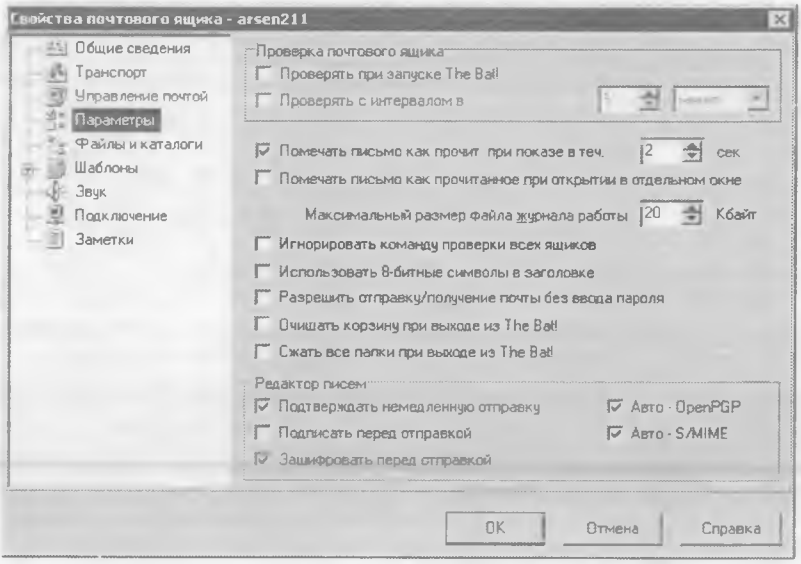

Рис. 6.4. Свойства почтового ящика

Чтобы включить режим шифрования, необходимо установить флажок Зашифровать перед отправкой.

Зашифрованное письмо можно отправить только тому получателю (получателям), для которого в адресной книге программы The Bat! указан сертификат или имеется ключ OpenPGP.

Использование в почтовых программах механизма шифрования намного повышает вероятность того, что пересылаемая информация не попадет в руки посторонних.

Хранение паролей

Логины, пароли, номера кредитных карт и подобная информация пользуются особым спросом у злоумышленников, и этот спрос постоянно растет. Поэтому для хранения подобной информации целесообразно использовать специальные программные средства. Для примера рассмотрим популярную утилиту Хранитель паролей.

Программу Хранитель паролей можно бесплатно скачать из Интернета по адресу http://olegprojects.narod.ru/downloads/PK.zip. Размер архива, предлагаемого для скачивания, достаточно небольшой: около 120 Кбайт. Рассмотрим порядок работы с программой Хранитель паролей на примере версии 2.6.

К достоинствам данной утилиты можно отнести то, что она является русскоязычной, проста в использовании и не требует инсталляции (следовательно, не оставляет следов в системном реестре). Для запуска программы достаточно активизировать исполняемый файл.

Следует учитывать, что для успешной работы программы необходимо наличие библиотеки Msvbvm60.dll. Эта библиотека присутствует на большинстве компьютеров, но в случае необходимости ее можно скачать с сайта программы.

Интерфейс Хранителя паролей представлен на рис. 6.5.

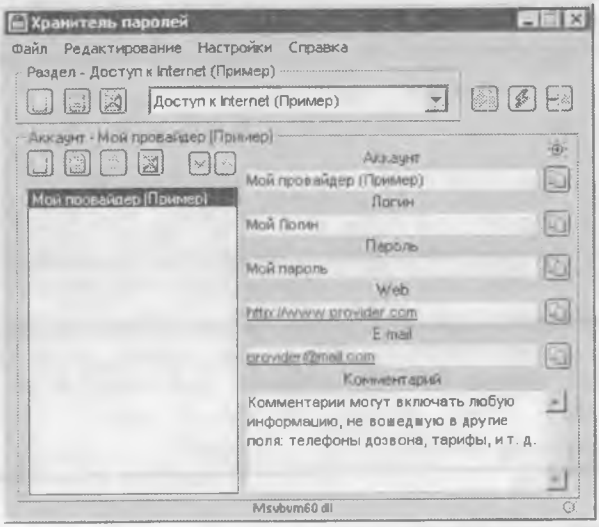

Рис. 6.5. Программа Хранитель паролей

Перед тем как приступить к использованию программы, рекомендуется просмотреть и при необходимости отредактировать параметры ее настройки. Для этого предназначены пункты меню Настройка. Подробно рассматривать все параметры нет необходимости: порядок работы с ними прост и интуитивно понятен. Отмечу лишь команду Настройки ▸ Безопасность ▸ Отключить/включить защиту от шпионов, предназначенную для защиты компьютера от клавиатурных шпионов. По умолчанию данный параметр включен, и его отключение целесообразно лишь при возникновении конфликтных ситуаций с автоматическими переключателями раскладок клавиатуры или антивирусными программами. Режим защиты компьютера от клавиатурных шпионов действует только при запущенной программе Хранитель паролей.

Утилиту можно поместить в автозагрузку, отобразить ее ярлык на Рабочем столе и включить в меню кнопки Пуск. Для этого предназначены соответствующие команды подменю Настройки ▸ Ярлыки.

Данные, хранящиеся в программе, целесообразно разместить в нескольких тематических разделах (например, Работа, Покупки, Развлечения и т. д.). Список разделов формируют и редактируют в верхней части окна. По умолчанию в программе создан демонстрационный раздел — Доступ к Internet (Пример) (см. рис. 6.5). Для добавления раздела нужно выполнить команду Редактирование ▸ Добавить раздел или нажать сочетание клавиш Ctrl+Insert. В результате на экране появится окно Добавление раздела, в котором с клавиатуры следует ввести произвольное название создаваемого раздела и нажать кнопку OK. Этот раздел будет добавлен в раскрывающийся список области Раздел.

В дальнейшем имя раздела можно отредактировать. Для этого предназначена команда Редактирование ▸ Редактировать раздел (можно также воспользоваться сочетанием клавиш Ctrl+Enter). Для удаления текущего раздела следует выполнить команду Редактирование ▸ Удалить раздел.

В каждом разделе можно создавать несколько учетных записей. На рис. 6.5 показано содержимое демонстрационной учетной записи Мой провайдер (Пример). Каждая запись может содержать информацию, например, об адресе электронной почты, кредитной карте или другую произвольную информацию. Для создания в выбранном разделе новой учетной записи нужно воспользоваться командой главного меню Редактирование ▸ Добавить аккаунт или нажать клавишу Insert. В результате на экране появится окно Добавление аккаунта,

в соответствующие поля которого следует с клавиатуры ввести имя учетной записи, логин, пароль, веб-адрес, адрес электронной почты и произвольный комментарий. После заполнения этих полей необходимо нажать кнопку OK. В результате созданная учетная запись будет добавлена в список выбранного в данный момент раздела.

Для перехода в режим редактирования учетной записи нужно выделить ее в списке и выполнить команду главного меню Редактирование ▸ Редактировать аккаунт (или нажать клавишу Enter). Чтобы удалить учетную запись, необходимо воспользоваться командой Редактирование ▸ Удалить аккаунт или нажать клавишу Delete.

При необходимости можно переместить учетную запись из одного раздела в другой. Для этого следует установить на нее курсор и выполнить команду главного меню Редактирование ▸ Переместить аккаунт (или нажать сочетание клавиш Ctrl+M). При этом на экране появится окно, в котором из раскрывающегося списка необходимо выбрать требуемый раздел и нажать кнопку OK.

Для защиты хранящихся в программе данных можно использовать пароль. Чтобы его задать, выполните команду Настройки ▸ Безопасность ▸ Пароль доступа к файлу данных. На экране появится окно, в котором следует с клавиатуры ввести пароль. Если вы хотите задать подсказку для пароля, то щелкните на ссылке Подсказка для пароля и в открывшемся окне с клавиатуры введите требуемый текст.

В программе реализована возможность автоматического генерирования паролей. Для перехода в соответствующий режим следует воспользоваться командой главного меню Файл ▸ Генератор паролей или нажать сочетание клавиш Ctrl+G. В результате откроется окно, изображенное на рис. 6.6.

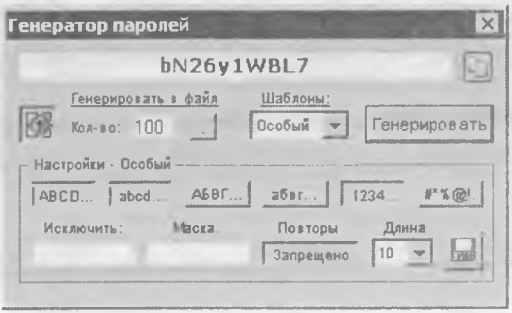

Рис. 6.6. Генератор паролей

С помощью генератора паролей можно автоматически создавать пароли различного уровня сложности. Требуемый уровень сложности выбирают из раскрывающегося списка Шаблоны: Слабый, Средний, Сильный или Особый. Чтобы запустить процесс генерирования, нажмите кнопку Генерировать. Дополнительные параметры можно настроить в области Настройки. Отображением этих параметров управляют с помощью кнопки со стрелкой, которая находится слева в верхней части окна (по умолчанию данные параметры не отображаются).

С помощью дополнительных параметров можно, например, ввести символы, которые нельзя будет использовать в паролях, задать маску генерируемого пароля, установить максимальное количество символов в генерируемом пароле и др. Чтобы быстро скопировать полученный пароль в буфер обмена, достаточно нажать кнопку, расположенную справа от поля с паролем.

Описание данной программы будет неполным, если не упомянуть еще об одной интересной функции – уничтожителе файлов и папок. С помощью уничтожителя можно оперативно удалить с компьютера ненужные файлы и папки без возможности восстановления. Для включения данного режима предназначена команда главного меню Файл ▸ Уничтожитель документов. После выполнения этой команды в правой части экрана отобразится небольшой значок с характерным рисунком. Чтобы удалить ненужный объект, достаточно просто перетащить его мышью на этот значок. Перед удалением на экране появится дополнительный запрос на подтверждение данной операции.

При необходимости данные, хранящиеся в программе, можно сохранить в виде отдельного файла. Для этого следует выполнить команду главного меню Файл ▸ Сохранить как и в открывшемся окне указать путь для сохранения.

Для сохранения базы данных программы в виде текстового файла предназначена команда главного меню Файл ▸ Экспорт в *.txt.

7. Восстановление системы

В процессе эксплуатации компьютера в работе операционной системы могут возникать различные сбои. Причины этих сбоев могут быть совершенно разные: внезапное отключение электроэнергии, аппаратные сбои, неквалифицированные действия пользователя, «засорение» системного реестра ненужными и устаревшими данными и т. д. Кроме этого, не стоит забывать о вредоносных программах, которые способны внести изменения в настройки или структуру системы.

В ранних версиях Windows (до Windows 2000) подобные проблемы можно было решить только переустановкой операционной системы. Однако в Windows 2000 и Windows XP существует специальная функция, с помощью которой можно вернуть стабильность работы системы без ее переустановки, — Восстановление системы.

Смысл восстановления системы заключается в ее откате к одному из предыдущих, более стабильных, состояний. При этом параметры и значения реестра, настройки операционной системы и другие данные восстанавливаются по состоянию на указанную дату.

В этом разделе рассмотрим процесс восстановления операционной системы на примере Windows XP.

При восстановлении системы нужно учитывать следующее.

- Восстановление системы впоследствии можно отменить.
- Перед восстановлением системы необходимо сохранить все нужные данные и закрыть работающие приложения.
- Процесс восстановления системы может занять продолжительное время, особенно на маломощных компьютерах.
- Восстановление системы предусматривает автоматическое завершение работы Windows и последующую перезагрузку компьютера. При загрузке будут использованы параметры настройки системы, соответствующие выбранной контрольной точке восстановления.

Если восстановление системы не решило проблему, можно выбрать более раннюю контрольную точку запустить процесс восстановления повторно.

Как работает средство Восстановление системы

Каким образом перейти в режим работы Восстановление системы и как определить, на какую дату необходимо выполнить восстановление операционной системы?

Для перехода в режим Восстановление системы следует выполнить команду Пуск ▸ Все программы ▸ Стандартные ▸ Служебные ▸ Восстановление системы. При этом на экране появится окно, изображенное на рис. 7.1.

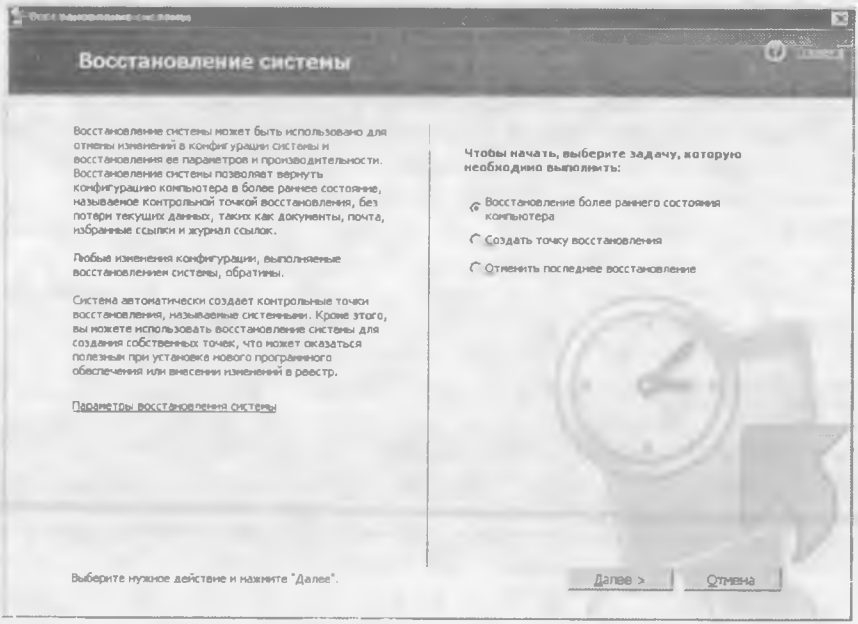

Рис. 7.1. Восстановление системы

В правой части этого окна с помощью переключателя следует выбрать требуемый режим работы: Восстановление более раннего состояния компьютера, Создать точку восстановления или Отменить последнее восстановление. Однако предварительно рекомендуется просмотреть и при необходимости изменить параметры восстановления системы. Для этого в левой части окна нужно щелкнуть на ссылке Параметры восстановления системы. При этом на экране появится окно Свойства системы с открытой вкладкой Восстановление системы (рис. 7.2).

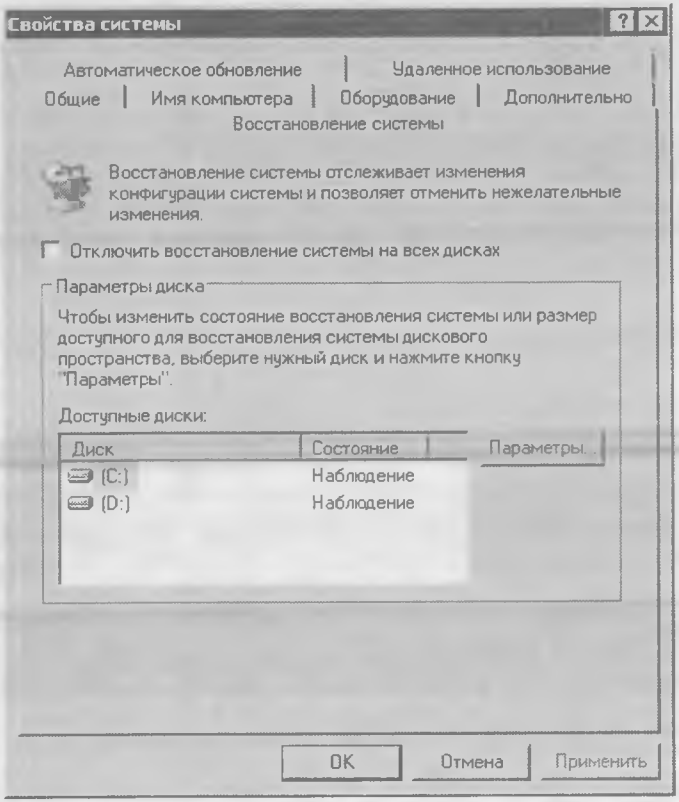

Рис. 7.2. Параметры восстановления системы

В данном окне путем установки соответствующего флажка можно отключить возможность восстановления системы. При этом система перестанет следить за изменениями на всех дисках компьютера.

На каждом локальном диске компьютера зарезервировано определенное количество дискового пространства для работы режима восстановления системы. По умолчанию на это выделяется 12 % дискового пространства. Чтобы изменить данное значение, необходимо на вкладке Восстановление системы выбрать нужный диск и нажать кнопку Параметры. Откроется окно Параметры диска, в котором с помощью соответствующего ползунка можно установить требуемое значение (от 1 до 12 %). Следует отметить, что уменьшение объема дискового пространства приведет к уменьшению

допустимого количества точек восстановления системы (подробнее о точках восстановления рассказано ниже, в соответствующем подразделе).

В окне Параметры диска можно отключить возможность восстановления системы на выбранном диске. Для этого достаточно установить флажок Отключить восстановление системы на этом диске.

Следует отметить, что отключить данную возможность на системном диске можно только после ее отключения на всех остальных локальных дисках компьютера.

Все изменения параметров на вкладке Восстановление системы (см. рис. 7.2) вступают в силу после нажатия кнопки Применить или ОК. С помощью кнопки Отмена можно выйти из данного режима без сохранения изменений.

Для запуска процесса восстановления системы в окне, изображенном на рис. 7.1, необходимо установить переключатель в положение Восстановление более раннего состояния компьютера и нажать кнопку Далее. В результате окно примет вид, показанный на рис. 7.3.

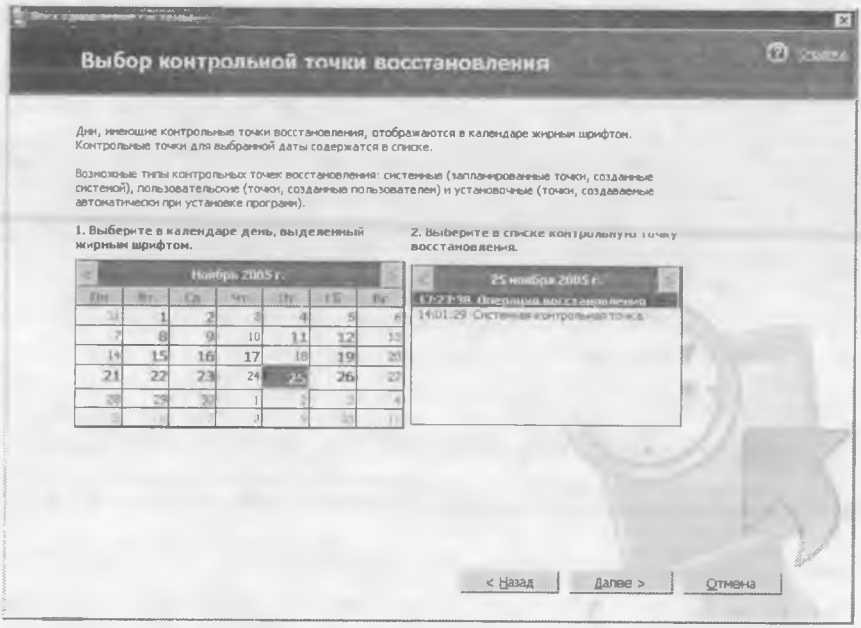

Рис. 7.3. Выбор точки восстановления

В данном окне необходимо выбрать контрольную точку восстановления системы (подробнее о точках восстановления и об их создании читайте ниже). Иначе говоря, здесь указывают дату и время, по состоянию на которые необходимо восстановить систему.

В расположенном слева списке перечислены даты текущего месяца. Если вы хотите перейти к предыдущему месяцу, нажмите кнопку со стрелкой, расположенную в левом верхнем углу списка. Для возврата к текущему месяцу предназначена аналогичная кнопка в правом верхнем углу списка. Даты, соответствующие контрольным точкам восстановления (на одну дату может приходиться несколько таких точек), выделены в списке полужирным шрифтом. Чтобы выбрать требуемую дату, установите на нее курсор (это возможно только для дат, которым соответствуют контрольные точки восстановления). При этом в расположенном справа списке отобразится список контрольных точек восстановления, приходящихся на эту дату, с точным временем и кратким названием (например, Системная контрольная точка). Чтобы выбрать точку восстановления, выделите ее в списке и нажмите кнопку Далее. При этом окно примет вид, показанный на рис. 7.4.

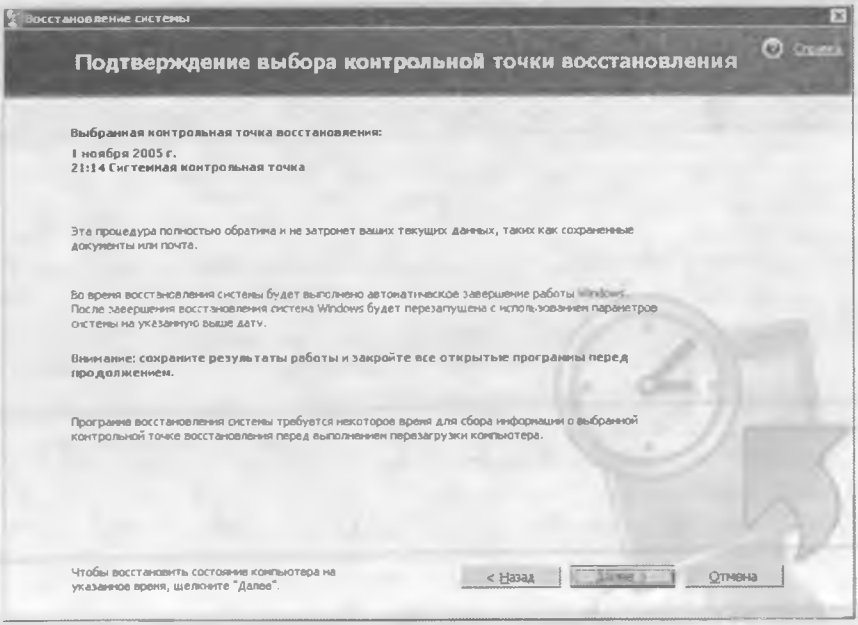

Рис. 7.4. Подтверждение точки восстановления

В данном окне следует просто подтвердить выбор точки восстановления. Для этого достаточно нажать кнопку Далее. Сразу после этого начнется процесс восстановления системы.

Процедура восстановления системы полностью обратима: ее всегда можно отменить. Для этого в окне, изображенном на рис. 7.1, следует установить переключатель в положение Отменить последнее восстановление и нажать кнопку Далее.

При восстановлении системы не будут затронуты имеющиеся данные: документы, электронная почта и т. д. Однако программы, которые были инсталлированы в промежутке времени между выбранной точкой восстановления и текущим моментом, возможно, придется переустановить. Это обусловлено, кроме всего прочего, тем, что в процессе восстановления системный реестр приводится в состояние, в котором он был на дату контрольной точки восстановления.

После нажатия в окне, изображенном на рис. 7.4, кнопки Далее процесс продолжится без участия пользователя. Будьте готовы к тому, что компьютер автоматически перезагрузится. Об окончании восстановления системы сообщит соответствующее информационное окно.

В следующем подразделе рассмотрим, как создать контрольные точки восстановления системы.

Контрольные точки восстановления

Контрольные точки восстановления системы бывают трех видов: системные, пользовательские и установочные.

Система автоматически создает контрольные точки восстановления через определенные интервалы времени в соответствии с установленным расписанием. Кроме того, они формируются перед установкой обновлений Windows XP (если вы используете систему автоматического обновления Windows XP), а также при первом включении компьютера после обновления операционной системы. Кроме этого, системная точка создается непосредственно перед восстановлением системы, а также перед отменой восстановления. Система также автоматически создает точки восстановления при инсталляции или удалении программ (в таких точках фиксируется состояние системы непосредственно перед инсталляцией или удалением).

Пользовательские контрольные точки можно создать самостоятельно, в любое нужное время. Для этого в окне, изображенном на

рис. 7.1, необходимо установить переключатель в положение Создать точку восстановления и нажать кнопку Далее. В результате окно примет вид, показанный на рис. 7.5.

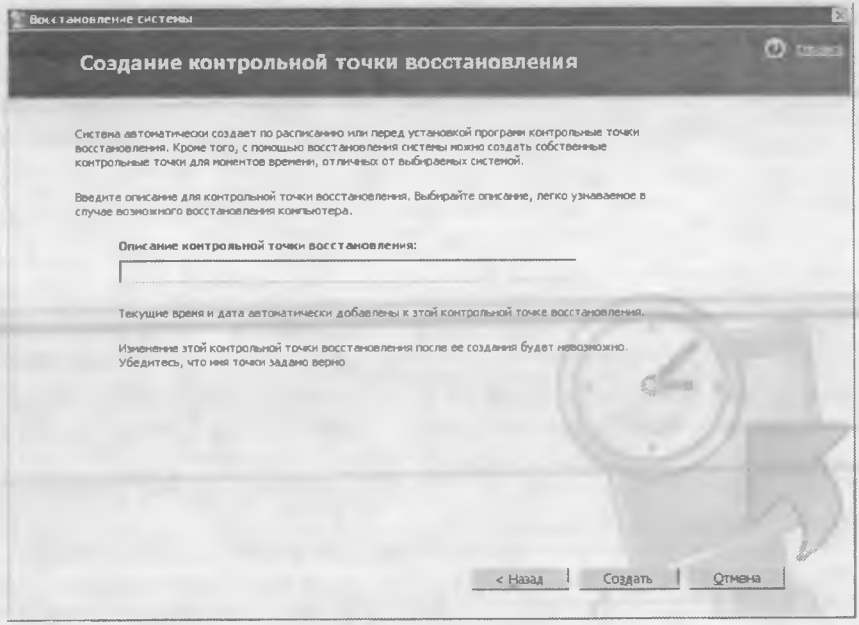

Рис. 7.5. Создание пользовательской точки восстановления

В поле Описание контрольной точки восстановления данного окна следует с клавиатуры ввести краткое наименование или описание создаваемой точки. К введенному значению автоматически будут добавлены текущие дата и время. Следует внимательно отнестись к заполнению этого поля, поскольку в дальнейшем изменить параметры контрольной точки восстановления будет невозможно.

После ввода описания создаваемой точки восстановления нажмите кнопку Создать. По истечении некоторого промежутка времени на экране появится сообщение о создании новой контрольной точки с указанием точных времени и даты, а также описанием (наименованием) контрольной точки.

Поскольку точки восстановления системы занимают определенное место на жестком диске компьютера, они периодически удаляются. Обычно это касается точек восстановления, созданных более

чем за три месяца до настоящего момента, однако если необходимо максимально освободить место на жестком диске, то можно удалить все точки восстановления за исключением последней. Для этого следует воспользоваться режимом очистки диска, вызываемым командой Служебные ▸ Очистка диска.

Отмена восстановления системы

Иногда бывает так, что восстановление системы не приносит желаемых результатов или в результате неудачно выбранной контрольной точки восстановления система начинает работать еще хуже. В таком случае можно отменить восстановление.

Данный процесс по сути представляет собой то же восстановление. При этом восстанавливаются все параметры и настройки системы, которые использовались до последнего восстановления.

Для отмены восстановления в окне, изображенном на рис. 7.1, необходимо установить переключатель в положение Отменить последнее восстановление, после чего нажать кнопку Далее. В окне появится информация о дате и времени отменяемого восстановления системы. Для запуска отмены восстановления следует нажать кнопку Далее.

После этого процесс отмены продолжится так же, как и процесс восстановления, — без участия пользователя. В нужный момент компьютер автоматически перезагрузится, а после окончания отмены восстановления на экране появится соответствующее информационное сообщение.

Отмечу, что выполненную отмену восстановления впоследствии также можно отменить.

8. Восстановление данных

Многие пользователи компьютера сталкивались с проблемой потери данных. Независимо от причины утраты информации (ошибочное удаление, действие вредоносной программы или что-то иное) в подобной ситуации обязательно возникает вопрос: можно ли как-нибудь восстановить данные? В этом разделе рассмотрим некоторые приемы и способы, которые помогут вернуть утраченную информацию.

Восстановление удаленных файлов

Процесс восстановления потерянного файла может зависеть от того, каким образом файл был удален.

Наиболее простой вариант — удаление в Корзину. В данном случае для восстановления файла достаточно найти его значок в Корзине, щелкнуть на нем правой кнопкой мыши и в открывшемся контекстном меню выбрать пункт Восстановить. В результате файл вернется на то место, откуда он был удален в Корзину.

Более сложная ситуация — удаление файла без участия Корзины (например, нажатием сочетания клавиш Shift+Delete) или в результате воздействия вируса. Однако и в этом случае данные не потеряны безвозвратно. Удаленные файлы можно восстановить как вручную, так и автоматически, с помощью специально предназначенных утилит. В этой книге не будем останавливаться на ручном восстановлении, так как это требует некоторых специфических знаний, а рассмотрим специализированные программы.

Почему же восстановление удаленных файлов возможно? Как поступить, если необходимо бесследно удалить конфиденциальную информацию?

Дело в том, что при удалении файлы не стираются с жесткого диска физически, а просто видоизменяются, в результате чего система распознает их как удаленные. Кластеры таких файлов считаются свободными, и, пока они не отданы другому файлу, восстановить удаленный файл несложно. Причем вероятность восстановления

удаленных файлов остается даже после того, как свободные кластеры перераспределятся.

Иначе говоря, в большинстве случаев удаленные файлы и папки можно вернуть. Нельзя восстановить данные только после полного форматирования диска.

Таким образом, любую конфиденциальную информацию, удаленную стандартными способами, в большинстве случаев можно без особых проблем восстановить и изучить. Для надежного удаления секретных данных следует использовать специально предназначенные программы, называемые «шредерами», «затирателями», «уничтожителями» и др. Не вдаваясь в технические подробности, отмечу, что принцип действия большинства таких программ заключается в многократном прописывании определенного кода в освободившиеся кластеры удаленного файла. После этого восстановить информацию практически нереально.

Большинство популярных утилит, предназначенных для восстановления удаленных файлов, англоязычные. Тем не менее они обладают достаточно простым и понятным интерфейсом, поэтому при использовании этих программ у вас не возникнет особых затруднений.

FileRecoveryAngel

Программа FileRecoveryAngel, с которой вы познакомитесь в данном подразделе, представляет собой утилиту для восстановления удаленных файлов. С ее помощью можно восстановить данные, удаленные не только с жесткого диска, но и с внешних носителей информации. Данную программу можно скачать в Интернете по адресу www.filerecoveryangel.com/downloads/setup.exe. Размер инсталляционного файла, предлагаемого к скачиванию, составляет примерно 700 Кбайт.

Рассмотрим утилиту FileRecoveryAngel на примере версии 1.13 — последней на момент написания книги.

Рабочее окно программы представлено на рис. 8.1.

В левой части окна отображается иерархический список дисков и папок, имеющихся на компьютере, в правой — содержимое диска, выбранного в левой части (включая удаленные файлы). Для каждого объекта в соответствующих столбцах показана следующая информация: имя и статус файла (восстановлению подлежат файлы со статусом Deleted (Удаленный)), а также размер и дата последнего изменения.

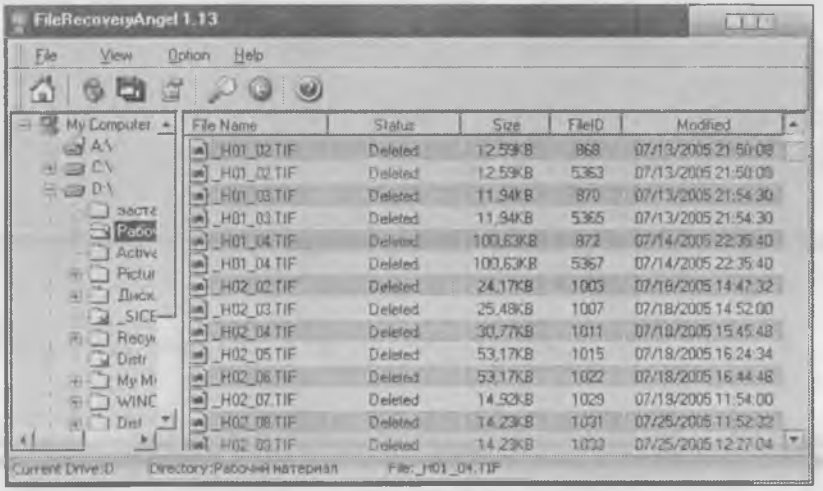

Рис. 8.1. Интерфейс программы FileRecoveryAngel

Для восстановления файла со статусом Deleted (Удаленный) необходимо установить на него курсор и выполнить команду главного меню File ▸ Recovery (Файл ▸ Восстановление) или аналогичную команду контекстного меню. При этом откроется окно Обзор папок. В данном окне необходимо выбрать папку, в которую будет помещен восстановленный файл. При этом нельзя выбрать диск, на котором находится удаленный файл, а также папку на этом диске. Иначе говоря, если удаленный файл находится на диске C:, то восстановить его можно на любой диск, кроме C:.

После окончания процесса восстановления файла на экране появится окно с соответствующим сообщением.

В программе реализована возможность поиска объектов. Для перехода в соответствующий режим следует выполнить команду главного меню Option ▸ Search (Выбор ▸ Поиск) или нажать соответствующую кнопку на панели инструментов.

При необходимости можно ознакомиться с подробной информацией о диске, выделенном в левой части окна программы. Для этого предназначена команда главного меню View ▸ Drive Information (Вид ▸ Информация о диске). При выполнении данной команды на экране появится окно, содержащее сведения о диске: имя, общее количество секторов и количество скрытых секторов, название используемой файловой системы и т. п.

Кроме этого, вы можете просмотреть информацию об объекте, выбранном в правой части окна. Для перехода в соответствующий режим необходимо выполнить команду главного меню View ▸ File Property (Вид ▸ Свойства файла).

Recover4all Professional

Программа Recover4all Professional также предназначена для восстановления удаленных файлов. Сайт программы — www.recover4all.com. Рассмотрим порядок работы с данной утилитой на примере версии 2.25.

Интерфейс программы Recover4all Professional представлен на рис. 8.2.

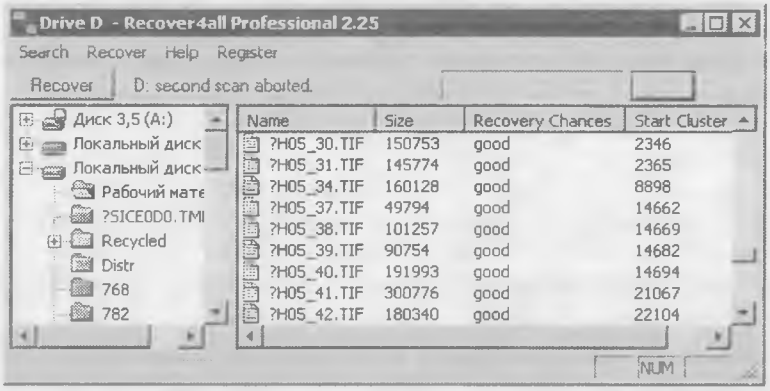

Рис. 8.2. Recover4all Professional

Рабочее окно Recover4all Professional разделено на две части: слева располагается иерархия имеющихся в компьютере дисков и папок, справа — содержимое диска или папки, выделенной в левой части окна.

Следует учитывать, что после запуска программы в левой части окна отображаются только используемые диски. Чтобы увидеть содержимое диска, необходимо щелкнуть на плюсике слева от названия нужного диска. После этого автоматически начнется процесс сканирования, который может занять продолжительное время. При необходимости сканирование можно прервать досрочно. Информация в правой части окна появится только после полного или частичного сканирования выбранного диска.

Чтобы приступить к восстановлению файла, сначала следует выделить его в списке. Если вы хотите выделить для последующего восстановления все имеющиеся в списке объекты, воспользуйтесь командой главного меню Recover ▸ Select all files in right pane (Восстановить ▸ Выбрать все файлы в правой части). Затем выполните команду главного меню Recover ▸ Recover selected files (Восстановить ▸ Восстановить выбранные файлы) или выберите в контекстном меню пункт Recover (Восстановить). При этом на экране появится окно, в котором нужно указать путь для восстановления. После нажатия в этом окне кнопки OK выбранный файл будет восстановлен и сохранен в указанное место.

«Ремонт» поврежденных файлов

В процессе работы файлы и папки могут не только случайно удалиться, но и повредиться. Поврежденный файл не исчезает, но в то же время работать с ним (читать, редактировать и т. д.) очень трудно или вообще невозможно.

Причины повреждения файлов могут быть самыми разными: от аппаратных сбоев до действия вредоносных программ. Однако результат в любом случае неприятен: если поврежденные файлы не получится восстановить, они будут безвозвратно утеряны.

Для восстановления поврежденных файлов рекомендуется использовать специально предназначенные утилиты, которые широко представлены в Интернете. Можно, конечно, попытаться сделать это вручную, но для этого необходимо обладать, во-первых, специфическими знаниями, а во-вторых, большим количеством времени.

Как отмечалось, в Интернете представлено множество программ, предназначенных для восстановления поврежденных файлов. Чтобы найти их, достаточно задать для поиска текст вроде Ремонт файлов утилиты (или что-то подобное). После этого останется лишь выбрать подходящую программу.

В этой книге рассмотрим две достаточно популярные программы, предназначенные для восстановления поврежденных файлов: BadCopy Pro и CDCheck.

BadCopy Pro

Одной из наиболее популярных программ, предназначенных для восстановления поврежденных файлов, является программа

BadCopy Pro. Программа условно бесплатная: ее демонстрационную версию можно скачать в Интернете по адресу http://download.jufsoft.com/download/badcopy3.exe. Размер дистрибутива, предлагаемого к скачиванию, составляет 851 Кбайт.

К достоинствам программы можно отнести ее широкую функциональность, а также большое количество поддерживаемых носителей информации: 3,5- и 5,25-дюймовые дискеты, компакт-диски и DVD, жесткие диски и др. К недостаткам — отсутствие русскоязычного интерфейса.

Рабочее окно программы показано на рис. 8.3.

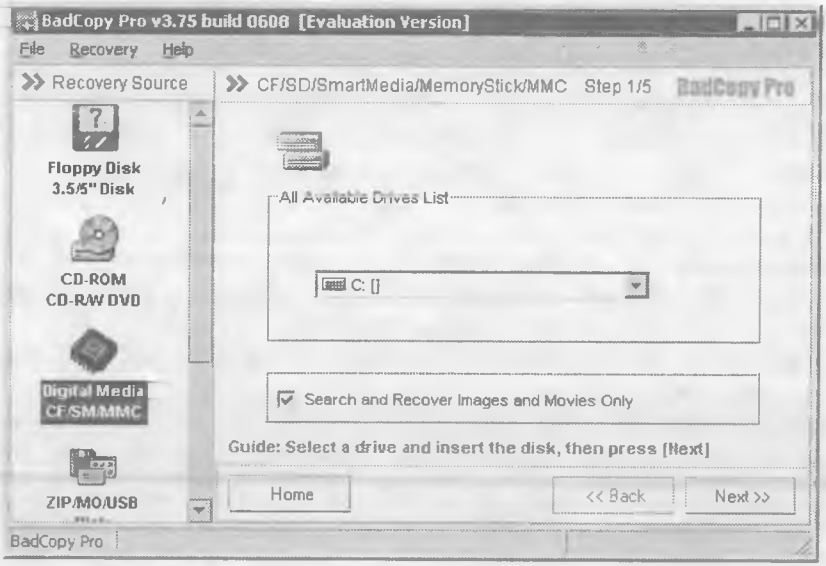

Рис. 8.3. Интерфейс программы BadCopy Pro

В левой части данного окна следует указать вид носителя информации (дискета, жесткий диск и т. д.). Если выбран жесткий диск, то в правой части окна из раскрывающегося списка выбирают название конкретного локального диска.

После этого следует нажать кнопку Next (Далее). Программа предложит выбрать способ восстановления файлов:

- Rescue Corrupted Files (Восстановить поврежденные файлы) — используют для восстановления файлов, которые отображают-

ся в окне Проводника, но недоступны для выполнения каких-либо действий;

- Rescue Lost Files — Mode #1 (Восстановить утраченные файлы — Способ 1) — применяют для восстановления файлов, которые не отображаются в окне Проводника и недоступны для работы;
- Rescue Lost Files — Mode #2 (Восстановить утраченные файлы — Способ 2) — используют в наиболее «тяжелых» случаях: программа применяет более сложные алгоритмы, повышающие вероятность удачного восстановления.

После выбора требуемого способа восстановления утилита начнет сканировать выбранный носитель информации. Результаты будут представлены в окне, которое показано на рис. 8.4.

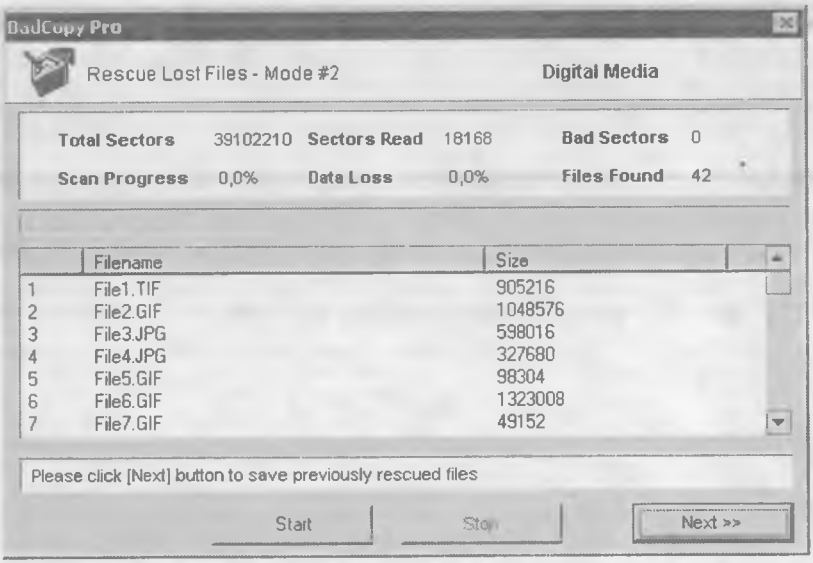

Рис. 8.4. Результаты сканирования

Следует отметить, что процесс сканирования может занять продолжительное время, особенно на маломощных компьютерах. При необходимости его можно прервать досрочно, нажав в окне, изображенном на рис. 8.4, кнопку Stop (Стоп).

После окончания процесса сканирования необходимо нажать кнопку Next (Далее). Откроется окно, изображенное на рис. 8.5.

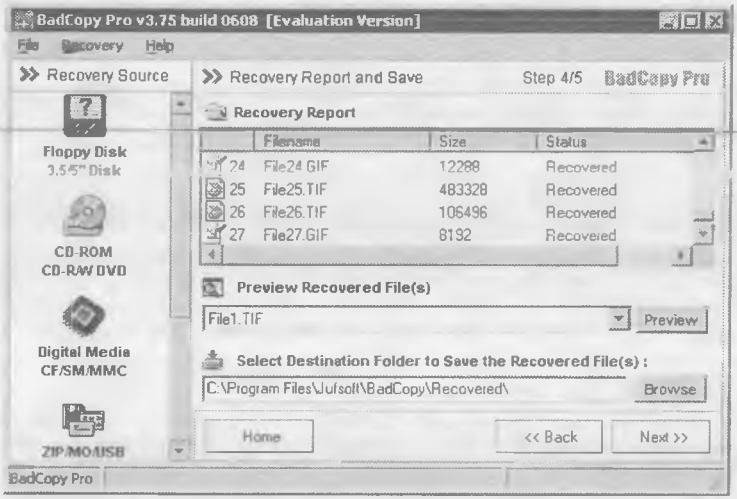

Рис. 8.5. Список файлов

В верхней части данного окна в поле Recovery Report (Отчет о восстановлении) перечислены объекты, обнаруженные в результате сканирования. Возможности программы позволяют просмотреть каждый объект. Для этого из раскрывающегося списка Preview Recovered File(s) (Предварительный просмотр восстановленных файлов) выберите требуемый файл и нажмите расположенную справа кнопку Preview (Предварительный просмотр). Содержимое файла отобразится в отдельном окне.

В нижней части окна в поле Select Destination Folder to Save the Recovered File(s) (Выберите путь к папке для сохранения восстановленных файлов) указывают путь к папке, в которой будет сохранен выбранный файл.

По умолчанию программа предлагает сохранить файл в папке Recovered (Восстановленные), которая расположена в каталоге программы. Этот путь можно изменить только с помощью расположенной справа кнопки Browse (Обзор). При нажатии данной кнопки на экране появится окно Обзор папок, в котором по обычным правилам Windows следует указать путь для сохранения.

Выделив файл, который необходимо восстановить, следует нажать кнопку Next (Далее). В результате восстановленный файл будет сохранен в указанной папке.

CDCheck

Рассмотрим небольшую утилиту, предназначенную для диагностики и восстановления поврежденных объектов. Данная программа работает со всеми версиями Windows. Бесплатно (для некоммерческого использования) утилиту CDCheck можно скачать в Интернете по адресу: http://www.elpros.si/CDCheck/CDCheckSetup.exe. Размер предлагаемого дистрибутива — 827 Кбайт. Программа поддерживает много языков, в том числе русский (однако справочная информация предоставляется только на английском языке).

Интерфейс программы представлен на рис. 8.6.

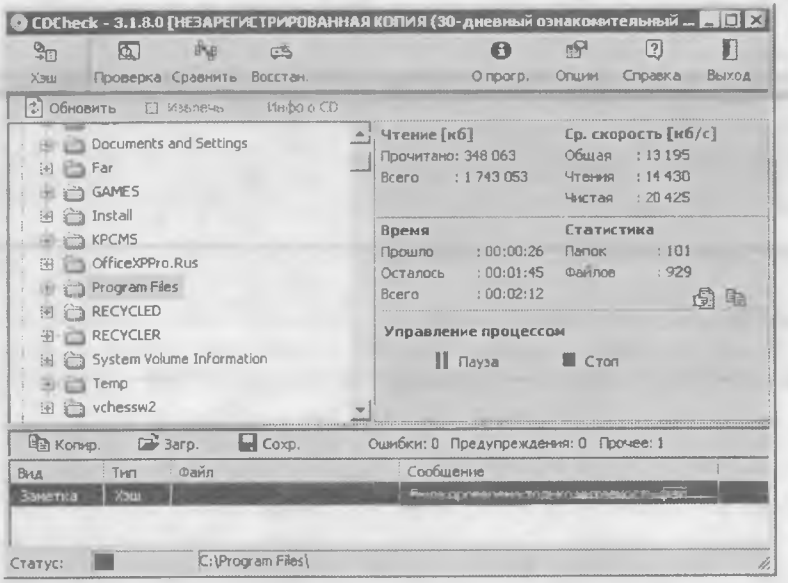

Рис. 8.6. Программа CDCheck

В левой части данного окна отображается иерархия дисков, папок и файлов. Для проверки определенного объекта следует выделить его и нажать кнопку Проверка, расположенную на панели инструментов.

Перед тем как приступить к использованию программы, рекомендуется просмотреть и при необходимости отредактировать ее параметры. Для перехода в соответствующий режим следует нажать

на панели инструментов кнопку Опции. В результате на экране появится окно, изображенное на рис. 8.7.

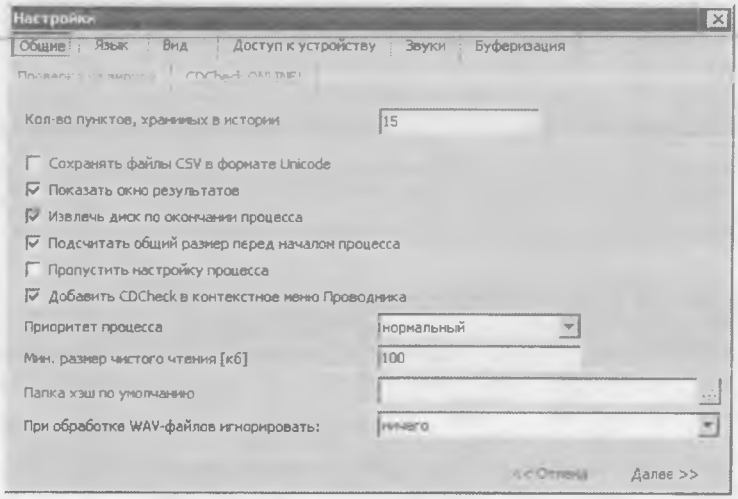

Рис. 8.7. Настройка программы CDCheck

В зависимости от функционального назначения параметры настройки программы сгруппированы на вкладках: Общие, Язык, Вид, Доступ к устройству, Звуки и Буферизация. Подробно рассматривать каждый из них не будем; остановимся лишь на некоторых параметрах.

При необходимости можно добавить команду вызова программы CDCheck в контекстное меню Проводника. Для этого на вкладке Общие (она открыта на рис. 8.7) нужно установить флажок Добавить CDCheck в контекстное меню Проводника (по умолчанию данный флажок установлен). Из раскрывающегося списка Приоритет процесса выбирают требуемый приоритет процесса сканирования: нет, низкий, ниже нормального, нормальный, выше нормального или высокий.

На вкладке Язык выбирают язык интерфейса. Для этого необходимо выделить требуемый язык (например, Russian (Русский)) и нажать кнопку Далее.

На вкладке Вид настраивают представление информации в окне программы. В частности, здесь указывают режим отображения статистики (Полная или Краткая), порядок расположения кнопок на панели инструментов (Вверху (как на рис. 8.6) или Слева) и др.

Параметры, расположенные на вкладке Звуки, позволяют настроить звуковое оформление при завершении работы программы и обнаружении первой ошибки. Путь к файлу звукового сигнала (этот файл должен иметь расширение WAV) указывают в соответствующих полях.

Как отмечалось, для запуска процесса проверки нужно выделить требуемый объект (диск, папку) и нажать кнопку Проверка. После нажатия данной кнопки на экране появится окно, в котором можно указать дополнительные параметры сканирования. Следует отметить, что сканирование может занять продолжительное время, особенно на маломощных компьютерах. Процесс проверки сопровождается демонстрацией статистической информации о ходе проверки. Эта информация отображается в правой части окна в информационных полях Чтение, Время, Статистика и Ср. скорость.

Область Управление процессом, расположенная под этими информационными полями, содержит две кнопки: Пауза и Стоп. С помощью кнопки Пауза можно временно приостановить процесс сканирования (после этого кнопка будет называться Далее). Кнопка Стоп предназначена для досрочного прекращения проверки.

Результаты проверки отображаются в окне Результат (рис. 8.8).

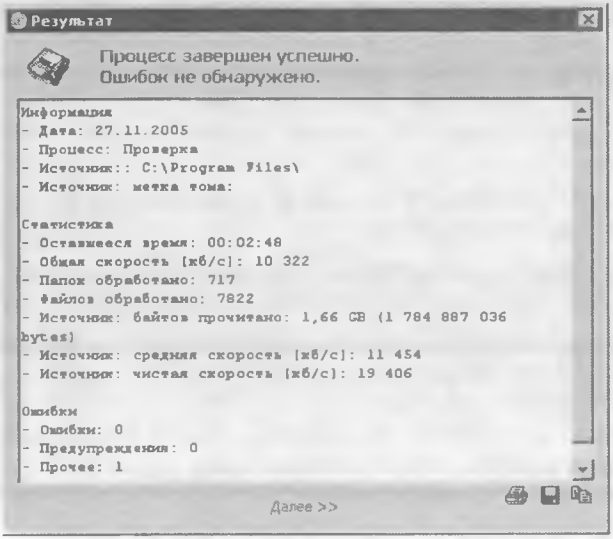

Рис. 8.8. Результат проверки

Для восстановления файла или папки необходимо воспользоваться соответствующей кнопкой на панели инструментов. При этом на экране появится окно настройки параметров восстановления. В данном окне указывают восстанавливаемый объект, путь для его сохранения и др. Для запуска восстановления следует нажать в данном окне кнопку Далее. После окончания процесса на экране появится окно с результатами, аналогичное окну, изображенному на рис. 8.8.

Резервное копирование данных

Всем известно, что для сохранения наиболее важных файлов и папок необходимо делать их резервные копии, причем желательно на других дисках. Однако в операционной системе Windows XP реализована штатная возможность архивации хранящихся на компьютере данных. С ее помощью при аварийном отказе системы вы сможете восстановить ее со всеми настройками.

Для перехода в рассматриваемый режим работы следует выполнить команду Пуск ▸ Все программы ▸ Стандартные ▸ Служебные ▸ Архивация данных. В результате на экране появится окно Мастера архивации или восстановления. Дальнейшие действия по созданию архивной копии данных следует выполнять в пошаговом режиме в соответствии с указаниями мастера.

На первом этапе с помощью соответствующего переключателя следует выбрать режим работы: Архивация файлов и параметров или Восстановление файлов и параметров. Выберите первый вариант, после чего нажмите кнопку Далее.

На втором этапе с помощью переключателя необходимо выбрать объекты для последующего архивирования.

- Мои документы и параметры настройки. При выборе этого варианта система будет архивировать данные пользователя, под учетной записью которого в текущий момент работает система (в том числе папки Мои документы, Application data и содержимое Рабочего стола).
- Документы и параметры настройки всех пользователей данного компьютера. Если переключатель установлен в это положение, то будут архивироваться данные всех пользователей компьютера.
- Всю информацию на данном компьютере. В этом случае будут архивироваться все данные, хранящиеся на всех локальных дис-

ках компьютера. При этом система создаст диск автоматического восстановления операционной системы.

- Предоставить возможность выбора объектов для архивации. При выборе этого варианта объекты для архивации нужно указать в окне, которое откроется после нажатия кнопки Далее (это окно отображается только при выборе данного варианта архивирования).

После выбора объектов нажмите кнопку Далее для перехода к следующему этапу.

В следующем окне мастера следует указать путь для архивирования и имя создаваемого архива (рис. 8.9).

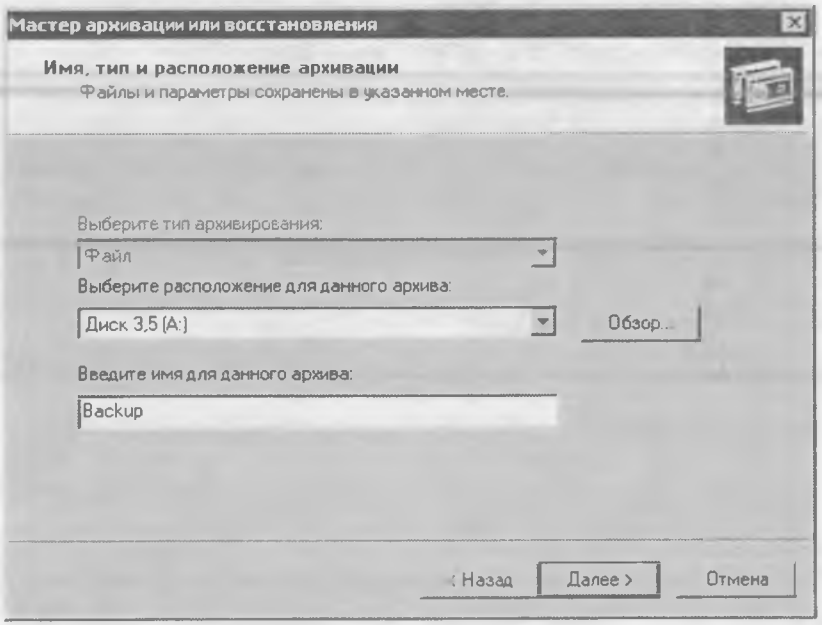

Рис. 8.9. Выбор пути и имени для архивируемого объекта

Расположение архива следует задать с помощью соответствующего раскрывающегося списка или кнопки Обзор, а имя нужно ввести в поле Введите имя для данного архива с клавиатуры.

После нажатия в данном окне кнопки Далее можно запустить процесс архивирования. Для этого на следующем этапе нужно нажать кнопку Готово. При необходимости можно настроить дополнительные

параметры архивирования: для этого следует нажать кнопку Дополнительно. В режиме дополнительной настройки указывают тип (обычный, добавочный и др.) и способ архивации (например, Проверять данные после архивации), определяют время начала архивации (Сейчас или Позднее (при выборе второго варианты нужно указать конкретное время для автоматической архивации)), а также задают иные параметры.

Чтобы восстановить архивированные данные, необходимо на начальном этапе работы Мастера архивации или восстановления выбрать режим Восстановление файлов и параметров и далее следовать указаниям мастера.

Как извлечь информацию с поврежденного жесткого диска

Большинству пользователей известно, что жесткий диск — не самое надежное место для хранения информации. Во-первых, он подвержен таким разрушающим факторам, как действие вредоносных программ и вирусов, неквалифицированные действия пользователей, аппаратные сбои и др. Во-вторых, жесткий диск, в отличие от компакт-дисков или других носителей информации, представляет собой механическое устройство, а, как известно, любой механизм рано или поздно изнашивается.

Поэтому ни один пользователь не застрахован от такой неприятности, как повреждение жесткого диска. В подобной ситуации самое главное — ни в коем случае не впадать в панику и не совершать необдуманных действий, поскольку это может только усугубить и без того сложную ситуацию. Не стоит забывать, что нередко данные, хранящиеся на поврежденном жестком диске, можно спасти.

Каким же образом можно попытаться спасти информацию? Конечно, самый простой способ — это обратиться к специалистам, которые сделают все возможное для спасения данных. Однако подобные услуги, как правило, стоят недешево, поэтому в некоторых случаях вполне можно обойтись собственными силами.

Самостоятельно восстанавливать информацию с поврежденного винчестера следует только пользователям, имеющим определенный опыт работы на компьютере. Новичкам для решения подобных проблем все же лучше обратиться к специалистам, поскольку неквалифицированные действия могут привести к окончательной и безвозвратной потере данных.

В настоящее время существуют различные способы восстановления информации с поврежденного жесткого диска. Большинство из них заключается в использовании специально предназначенных программ. В данном подразделе вы познакомитесь с одной из наиболее популярных программ такого типа — PC Inspector File Recovery. Рассмотрим ее на примере версии 4.0 — последней на момент написания книги.

Программа PC Inspector File Recovery представляет собой утилиту, предназначенную для восстановления информации с поврежденных жестких дисков. Данная программа распространяется бесплатно, ее можно скачать в Интернете: http://download.pcinspector.de/pci_filerecovery.exe. К скачиванию предлагается инсталляционный файл размером 5,9 Мбайт.

Ни в коем случае не следует устанавливать программу на тот диск, с которого нужно восстановить данные. Программа должна быть установлена на другом, отдельном жестком диске.

Программа мультиязычная, наряду с несколькими другими языками она поддерживает и русский. Следует учитывать, что перед инсталляцией программа предложит выбрать язык установки, но среди предлагаемых языков русского не будет. Поэтому для установки следует выбрать какой-либо другой язык (например, английский). Однако при каждом запуске программы на экране будет появляться окно со списком возможных языков интерфейса (рис. 8.10), среди которых будет русский язык.

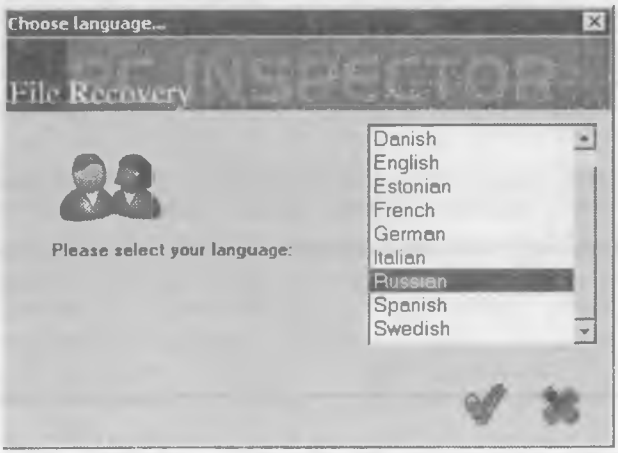

Рис. 8.10. Выбор языка интерфейса

Следует отметить, что справочная система программы русский язык не поддерживает.

В программе отсутствуют стандартные кнопки типа OK и Отмена. Вместо них на соответствующих кнопках изображены «галочка» (OK) и «крестик» (Отмена) (см. рис. 8.10).

После выбора языка программа предложит выбрать один из трех возможных режимов работы (рис. 8.11).

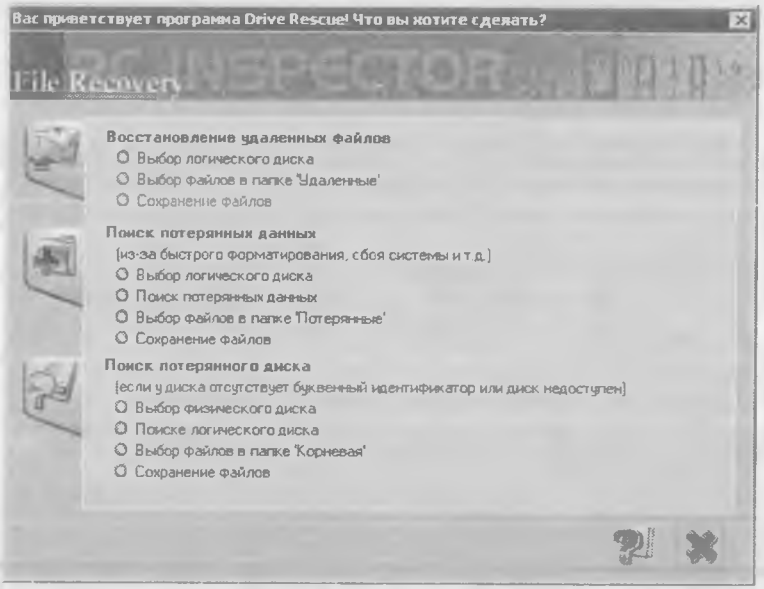

Рис. 8.11. Выбор режима работы

Режим Восстановление удаленных файлов предназначен для восстановления данных, которые были удалены пользователем, минуя Корзину (следовательно, PC Inspector File Recovery можно использовать в случаях, описанных в подразд. «Восстановление удаленных файлов»).

В режиме Поиск потерянных данных можно восстановить информацию, которая была утеряна, например, в результате повреждения файловой системы, быстрого форматирования диска и в иных подобных случаях. Этот режим работы наиболее востребован большинством пользователей.

Режим Поиск потерянного диска используется для поиска логических дисков, которые по каким-то причинам не видны в операционной системе, а также для восстановления информации с этих дисков.

После выбора режима работы начнется процесс сканирования, в результате чего на экране отобразится список логических дисков. В этом списке двойным щелчком выберите диск, данные которого необходимо восстановить. Сразу после этого начнется процесс сканирования выбранного диска, который, в зависимости от объема диска и технических характеристик компьютера, может занять от 5 до 40 мин. Результаты сканирования отобразятся в окне, показанном на рис. 8.12.

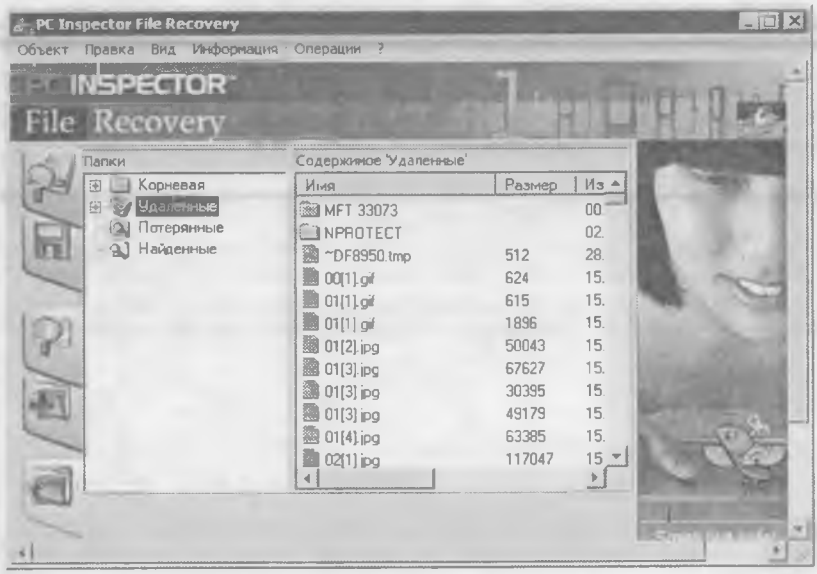

Рис. 8.12. Результаты сканирования диска

Файлы и папки, обнаруженные в результате сканирования, размещены в разделах Корневая (содержимое сканированного диска), Удаленные (удаленные пользователем файлы и папки), Потерянные и Найденные. В правой части окна отображается содержимое раздела, выбранного в левой части (например, на рис. 8.12 показано содержимое раздела Удаленные).

Для восстановления файла или папки нужно выделить его, после чего в контекстном меню выбрать пункт Сохранить в. При этом на экране появится окно, в котором указывают путь для сохранения. Настоятельно рекомендуется сохранять данные на другом диске, иначе они могут быть утеряны.

Кроме сохранения, контекстное меню содержит также еще несколько пунктов. С их помощью можно перейти в режим просмотра свойств выбранного объекта, переименовать выбранный объект, а также просмотреть его содержимое в шестнадцатеричном или текстовом формате.

В программе реализована возможность поиска данных. Для этого следует воспользоваться командой главного меню Объект ▸ Найти или щелкнуть на соответствующем значке, расположенном в левой части окна (см. рис. 8.12). При этом на экране появится окно настройки параметров поиска, в котором следует указать имя искомого объекта или задать маску поиска, после чего запустить процесс поиска с помощью соответствующей кнопки. Результаты поиска будут отображены в разделе Найденные окна, показанного на рис. 8.12.

Следует учитывать, что при восстановлении данных с испорченных жестких дисков независимо от используемого метода положительные результаты не гарантированы. Не исключено, что восстановленные и сохраненные в указанном месте объекты будут работать некорректно. Однако во многих случаях грамотное восстановление данных с поврежденных жестких дисков бывает успешным.

Заключение

Для успешной работы на компьютере, и особенно в Интернете, сегодня недостаточно просто иметь соответствующие навыки. В большой степени результаты работы зависят от того, насколько хорошо пользователь умеет защищать свой компьютер и хранящуюся в нем информацию. Вопрос защиты данных становится все более актуальным, так как современные мошенники постоянно совершенствуют свое «мастерство» и потеря бдительности может привести к весьма печальным последствиям.

В книге подробно рассмотрены различные ситуации, которые могут возникать при работе на компьютере, проанализированы их причины и даны советы и рекомендации по решению этих проблем. Особое внимание уделено опасностям, которые подстерегают пользователя при работе в Интернете, а также способам восстановления операционной системы и потерянных данных.

Изучение этой книги позволит читателям в короткие сроки научиться защищать информацию от ошибок, сбоев и злоумышленников.

Д. Донцов

Как защитить компьютер от ошибок, вирусов, хакеров

Заведующий редакцией	*Д. Гурский*
Руководитель проекта	*Е. Каляева*
Литературный редактор	*А. Алехна*
Художник	*К. Радзевич*
Корректоры	*Т. Курьянович, Е. Павлович*
Верстка	*В. Поживилко*

ООО «Питер Пресс», 198206, Санкт-Петербург, Петергофское шоссе, д. 73, лит. А29.
Налоговая льгота – общероссийский классификатор продукции ОК 005-93, том 2; 95 3005 – литература учебная.

Подписано в печать 04.09.06. Формат 60×90/16. Усл. п. л. 9.
Доп. тираж 4000 экз. Заказ № 2766.

Отпечатано с готовых диапозитивов в ООО «Типография Правда 1906».
195299, Санкт-Петербург, Киришская ул., 2.
Тел.: (812) 531-20-00, (812) 531-25-55.