Оглавление

Введение

Современный человек уже не может представить свою жизнь без компьютера. С каждым днем растет количество информации, которую мы доверяем своему электронному другу.

Однако не стоит забывать, что никто не может стопроцентно гарантировать сохранность имеющихся в компьютере данных. Причин, по которым они могут быть утеряны или испорчены, существует великое множество: беспечность и ошибочные действия пользователей, аппаратные сбои, внезапное отключение электричества, деятельность вредоносных программ, нестабильная работа операционной системы и т. д.

После утраты данных многие впадают в отчаяние, полагая, что восстановить их нереально. Однако это далеко не так, более того — как показывает практика, в большинстве случаев восстановить потерянную информацию можно. Самое главное — не паниковать: одной из наиболее распространенных ошибок является то, что пользователи, обнаружив потерю или порчу данных, начинают совершать массу необдуманных действий, лишь усугубляя тем самым и без того непростую ситуацию.

Иногда восстановить информацию можно штатными средствами операционной системы, но чаще для этого придется прибегнуть к помощи специально предназначенных программ. Конечно, в настоящее время есть и немало специализированных фирм, которые занимаются восстановлением утраченных данных — но зачем же платить деньги за то, что можно сделать самостоятельно? Прочитав эту книгу, вы убедитесь, что это не так сложно, как может показаться на первый взгляд.

Но вначале мы проанализируем основные причины, приводящие к потере информации. Об этом, а также о профилактических мерах, позволяющих сберечь хранящиеся в компьютере данные, пойдет речь в первой главе книги.

Глава 1. ОСНОВНЫЕ ПРИЧИНЫ, ПРИВОДЯЩИЕ К ПОТЕРЕ ДАННЫХ

Итак, какие же причины чаще всего становятся причиной потери или порчи хранящихся в компьютере данных? Об этом читайте в нижеследующих разделах книги.

1.1. Выход из строя аппаратной части компьютера

Аппаратные сбои способны привести к полной или частичной потере данных: например, из-за неисправного блока питания может «сгореть» жесткий диск со всем его содержимым. В этом разделе мы расскажем о том, какие компоненты аппаратной части компьютера являются наиболее уязвимыми.

В первую очередь поломкам подвержены блок питания, жесткий диск и материнская плата. Могут возникать проблемы с оперативной памятью, однако здесь дело может быть и не в самой «оперативке», а в других нюансах — например, в результате попадания пыли могут пропадать контакты. В последнем случае пользователь может самостоятельно устранить проблемы (при том условии, что он знает, где в системном блоке находится оперативная память, и каким образом ее нужно снимать и устанавливать). Для этого нужно снять оперативную память, и осторожно протереть ее (особенно контактную группу) куском мягкой сухой материи, после чего вернуть на свое место.

Если возникают проблемы с аппаратной частью компьютера, то сразу после его включения об этом может просигнализировать BIOS. Для каждой нештатной ситуации в нем предусмотрен набор определенных звуковых сигналов. Если проблем нет, то любой BIOS выдает один короткий сигнал; остальные сигналы могут различаться в зависимости от модели BIOS: например, один длинный и три коротких звуковых сигнала в AwardBIOS означает наличие проблем с клавиатурой, а в AMIBIOS или в PhoenixBIOS сигнализирует об ошибке оперативной памяти.

Если полностью выходит из строя блок питания, то компьютер включить не удастся. Однако в большинстве случаев он ломается не моментально. Перед этим можно заметить признаки нестабильности в работе — в частности, 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 проявление дополнительных симптомов: заметное падение быстродействия работы компьютера, увеличение шума, издаваемого жестким

диском, возникновение ошибок при чтении файлов. Если имеет место 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.

Вообще жесткий диск, как известно, представляет собой своеобразное хранилище всех данных, находящихся в компьютере. Если при повреждении или выходе из строя любого другого оборудования (оперативной памяти, материнской платы и др.) риск утраты информации не очень велик, то с жестким диском ситуация такова: если он поврежден, либо сбилась его разметка, то вся хранящаяся на нем информация (как операционная система, так и всевозможные файлы и приложения) скорее всего будет утеряна.

Тем не менее, можно попытаться восстановить хотя бы часть информации. При этом необходимо учитывать, что процесс восстановления может быть достаточно трудоемким, а получение положительного результата не гарантируется.

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 поломки. При частичных поломках нередко сохраняется возможность продолжения работы — это касается, например, неисправности некоторых портов. Если же материнская плата полностью выходит из строя (например, перегорела в результате перепадов напряжения), то работа на компьютере становится невозможной. Настоятельно рекомендуется при возникновении подозрений о частичном выходе из строя материнской платы провести диагностику и устранить неисправности (вплоть до замены материнской платы), так как в некоторых случаях частичный выход из строя материнской платы может привести к поломкам и другого оборудования — в частности, процессора и оперативной памяти.

1.2. Проблемы с электроснабжением

Любой пользователь компьютера должен учитывать, что отечественная электроэнергия отличается невысоким (мягко говоря) качеством. Это относится не только к Российской Федерации, но и практически ко всем странам СНГ. На первый взгляд это незаметно, и многие могут задать вопрос: как же так — оказывается, сколько живем, столько и пользуемся некачественной электроэнергией?

Дело в том, что персональный компьютер представляет собой гораздо более тонкий механизм, чем остальная техника. И перепады напряжения в электрической сети, не имеющие никаких последствий,

например, для холодильника или телевизора, могут в то же время привести к серьезной поломке компьютера. Причем для их возникновения необязательно наличие каких-то видимых причин вроде природных катаклизмов (например, грозы) или внезапно включенной соседом электродрели — скачки напряжения в наших сетях могут происходить и сами по себе.

Следует отметить еще и то, что электропроводка в подавляющем большинстве домов (опять же, речь идет о территории СНГ), безнадежно устарела и морально, и физически (в частности, заземление имеется только в новых домах; в зданиях же «советской постройки» такой «роскоши» не предусмотрено).

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 в то время 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 в квартире, а сейчас многие имеют по два (а то и три) телевизора. Плюс к этому, многие сегодня имеют различного рода электрочайники-обогреватели-микроволновки и т. д. Это какая же нагрузка ложится на сеть, проложенную в 60–80-х годах! Поэтому многим известна примерно такая ситуация — сосед включил электрочайник (или обогреватель), и по всему «стояку» в подъезде отключился свет.

Разумеется, подобные «электрические» приключения не могут проходить бесследно для персонального компьютера, а в некоторых случаях они просто губительны. И если в результате проблем с электропитанием оказалась утеряна только информация, введенная в последнем сеансе 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 даже более ощутимо).

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

В первую очередь отметим, что ни в коем случае нельзя включать компьютер (а также — монитор) 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 его приходится приобретать отдельно. Сетевой фильтр внешне представляет собой обычный «трой-

ник»-удлинитель (только гнезд в нем не три, а четыре или пять), снабженный 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 с электропитанием рекомендуется использовать специальный прибор — источник бесперебойного питания. Его характерной особенностью является то, что компьютер питается именно от него, а не непосредственно из сети. Иначе говоря, источник бесперебойного питания — это своеобразный буфер между электрической сетью и компьютером. В его состав, помимо прочего, входит аккумуляторная батарея (перед первым использованием ее нужно заряжать примерно 4–6 часов; подробно об этом рассказывается в руководстве пользователя), 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.

Кроме этого, источник бесперебойного питания «сглаживает» любые перепады напряжения в сети, защищая тем самым персональный компьютер от связанных с этим поломок. Следует отметить, что многие ИБП защищают также и модем — от перепадов напряжения в телефонной сети. Для этого в таких ИБП 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 его техническими характеристиками, а именно — подходит ли он к конкретному компьютеру. Не рекомендуется приобретать источник бесперебойного питания с рук либо на рынке.

1.3. Уязвимость программной части компьютера

Несмотря на то, что аппаратные сбои способны принести пользователю немало проблем, большинство уязвимых мест компьютера содержится все же в его программной части. Их возникновение обусловлено целым рядом факторов: неквалифицированные либо ошибочные действия пользователя, конфликтные ситуации, возникающие между разными приложениями либо приложением и операционной системой, нестабильная работа операционной системы, программные ошибки (от которых не застраховано ни одно приложение), действия вредоносных программ (вирусов, троянов и т. п.) и др.

Какие же программные места компьютера наиболее уязвимы?

Если говорить об операционной системе Windows, то в первую очередь следует отметить системный реестр. В немалой степени его уязвимость обусловлена тем, что многие пользователи в стремлении оптимизировать работу системы, настроить ее под себя, ускорить быстродействие, «догнать и перегнать» и т. п. проводят с ним всевозможные эксперименты, что в конечном итоге нередко приводит к прямо противоположному результату.

Кроме этого, в системном реестре регистрируются многие устанавливаемые на компьютер приложения. Поэтому при удалении программ с компьютера следует не просто удалить соответствующую папку из каталога **Program Files** (или другого места, где установлено приложение), а воспользоваться специально предназначенной функциональностью, вызов которой осуществляется с помощью команды **Пуск ⇒ Панель управления ⇒ Установка и удаление программ**. Хотя 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. Чтобы избежать подобных неприятностей, рекомендуется периодически проводить чистку системного реестра. Разумеется, это делается не вручную, а с помощью специально разработанных программ и утилит, которых в настоящее время имеется великое множество. Они могут быть платными, условно-платными и бесплатными, большинство из них можно скачать в Интернете.

Как правило, нестабильная работа операционной системы обычно проявляется после продолжительного ее использования. При этом в работе системы могут возникать различного рода сбои, существенно уменьшается ее быстродействие, а место, занимаемое системной папкой на жестком диске, может быть значительно больше обычного; в конечном итоге в какой-то момент система может вообще не загрузиться.

Вообще следует отметить, что операционные системы семейства Windows достаточно уязвимы. Но это связано в первую очередь не с какими-то их конструктивными недостатками, а с тем, что ввиду широкой распространенности они хорошо изучены вирусописателями, хакерами, взломщиками и т. п. «деятелями». Поэтому корпорация Microsoft вынуждена периодически выпускать различного рода «заплатки» для повышения защищенности системы. Кстати, одним из наиболее опасных явлений является проникновение в компьютер удаленных злоумышленников через Интернет; более подробно об этом мы поговорим ниже, в разделе «Незащищенность компьютера от проникновения извне».

Операционные системы UNIX и Linux с точки зрения защищенности выглядят более предпочтительно (в первую очередь потому, что

они не так досконально изучены злоумышленниками). Однако в настоящее время они не получили такого широкого распространения, как системы семейства Windows.

К достаточно уязвимым приложениям можно отнести интернет-обозреватель Internet Explorer и почтовые программы Microsoft Outlook и Outlook Express. Причины их уязвимости те же, что и в операционной системе Windows — они широко распространены и хорошо изучены как пользователями, так и распространителями вредоносных программ. В настоящее время распространены также интернет-обозреватели Opera, Mozilla и др.; они имеют не меньше уязвимых мест, чем Internet Explorer, но ввиду слабой изученности считаются более надежным с точки зрения безопасности.

Помимо перечисленного, в программной части компьютера могут возникать различного рода программные ошибки по причине того, что разные приложения могут пользоваться одними и теми же библиотеками, ресурсами и др., что нередко приводит к конфликтам, которые могут закончиться потерей данных. Чем больше на компьютере установлено приложений и программ, тем больше вероятность возникновения различного рода конфликтных ситуаций. При этом следует учитывать, что некоторые современные приложения корректно работают только при соблюдении определенной конфигурации оборудования.

Ну и, конечно, следует проявлять разборчивость при инсталляции приложений и не устанавливать на свой компьютер все, что попало. Особенно это касается продуктов, распространяемых бесплатно.

Говоря о возможных программных сбоях, нельзя не упомянуть о таком явлении, как компьютерные вирусы. Наверное, сегодня нет ни одного пользователя компьютера, который о них бы не слышал.

Компьютерный вирус — это вредоносная программа, проникающая в компьютер и выполняющая в нем определенные действия без ведома пользователя, хотя, возможно, и при невольном его содействии. Заразиться вирусом можно где угодно — в Интернете, в локальной сети, с дискеты или компакт-диска и др.

Внимание. *Традиционно наиболее «заразными» местами считаются: развлекательные сайты «пикантной» направленности (проще говоря, порносайты), и компьютеры, установленные в общественных местах — например, в институте для студентов либо для клиентов на почте (за день таким компьютером воспользуется с десяток посетителей, и каждый придет со своей дискетой, на которой может быть неизвестно что записано)*.

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. Поэтому необходимо пользоваться надежной антивирусной программой и следить за актуальностью сигнатурных баз.

1.4. Небрежность и неквалифицированные действия пользователей

Наверное, ни один вирус и никакой перепад напряжения в сети не могут причинить такого ущерба компьютеру и хранящейся в нем информации, который могут вызвать неквалифицированные действия пользователя либо элементарная небрежность. Такие действия можно условно разделить на четыре группы:

- неквалифицированное редактирование системного реестра;
- неквалифицированное редактирование системных и загрузочных файлов;
- попытка самостоятельно починить компьютер (или изменить параметры его работы) путем проникновения внутрь системного блока (иначе говоря, всякие эксперименты с «железом»);
- неаккуратность в обращении (случайное отключение питания, нечаянное удаление файлов и т. п.).

Кратко проанализируем каждую из них.

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

Эта возможность реестра как магнитом притягивает к себе многих пользователей. Начинаются всевозможные эксперименты, как путем ручного редактирования реестра, так и с помощью различного рода сомнительных утилит, которых в Интернете имеется великое множество. Нередко в конечном итоге реестр приходит в такое состояние, что система просто отказывается загружаться, либо начинает работать очень нестабильно.

Внимание. *Если уж очень хочется поэкспериментировать с реестром, то, по крайней мере, нужно хотя бы сохранить его резервную копию, причем не только на жестком диске, но и на внешнем носителе информации. Для этого в окне редактора реестра предназначена команда главного меню* ***Файл ⇒ Экспорт*** *(при этом курсор должен быть установлен в корневую позицию иерархии реестра). При активизации команды на экране открывается окно* ***Экспорт файла реестра****, в котором по обычным правилам Windows следует указать путь для сохранения. Но в любом случае без крайней нужды вносить изменения в системный реестр категорически не рекомендуется.*

Непозволительные вольности с реестром часто приводят к тому, что приходится переустанавливать операционную систему.

Однако в последних версиях Windows (начиная с 2000) реализована функциональность, позволяющая «откатить» настройки операционной системы к какому-либо из предыдущих состояний. Она называется **Восстановление системы**; чтобы перейти в режим работы с ней, следует воспользоваться командой **Пуск ⇒ Все программы ⇒ Стандартные ⇒ Служебные ⇒ Восстановление системы**. С помощью данной функциональности восстанавливается состояние системы, зафиксированное в определенной точке восстановления на установленную дату (эти точки создаются как вручную, так и автоматически). Подробное описание данного процесса приводится ниже, в следующей главе. Здесь же мы отметим, что, конечно, восстановление системы позволяет избавиться от многих искусственно созданных проблем, но если операционная система отказывается загружаться, то это средство уже не поможет.

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

Внимание. *В большинстве современных файловых менеджеров (Total Commander, Far и др.) имеется режим отображения информации, при использовании которого системные и загрузочные файлы не показываются. Настоятельно рекомендуется включить этот режим, чтобы не было соблазнов поредактировать такие файлы*.

Что побуждает пользователя редактировать системные и загрузочные файлы? Да 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 Windows.

Многие пользователи, едва купив компьютер и нахватавшись поверхностных знаний об его устройстве, начинают считать себя великими специалистами в этом вопросе. При этом 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 другом компьютере, может отказаться работать на компьютере пользователя именно потому, что она несовместима с установленным на нем оборудованием.

Ну а что касается небрежности пользователей — то здесь дать какой-то совет сложно: многие становятся внимательными только после того, как пару раз по причине своей беспечности потеряют жизненно важную информацию. Остается лишь напомнить азбучную истину: все важные данные необходимо хранить не только в компьютере, но и на внешних носителях.

1.5. Незащищенность компьютера от проникновения извне

Одним из важнейших условий обеспечения сохранности информации является защищенность компьютера от любого проникновения извне.

Пока вы спокойно работаете в Интернете, не думая ни о чем плохом, у вас могут красть секретную информацию, внедрять в компьютер программы-шпионы (так называемые SpyWare), удалять данные с жесткого диска или просто портить их — и все это совершенно незаметно от вас. Кто-то занимается подобными вещами просто от нечего делать, но в последнее время нередки случаи, когда подобные действия осуществляются с целью наживы путем мошенничества.

Совет. *Даже если вы завершили работу и выключили компьютер, обязательно физически отключите его от Интернета путем отсоединения кабеля. Помните, что современные злоумышленники умеют проникать даже в неработающие компьютера с целью хищения, порчи или удаления информации*.

Характерный пример — удаленное шифрование данных. Смысл этого способа заключается в том, что злоумышленник, получив доступ к удаленному компьютеру, шифрует в нем определенные файлы, документы и т. п. таким образом, что пользователь не может их самостоятельно расшифровать. Через определенное время пользователь зараженного компьютера получает электронное письмо с требованием перевести определенную сумму денег (это может быть и 200, и 20000 долларов, и любая другая сумма) по указанным реквизитам — за это ему будет выслан ключ для расшифровки информации. Разумеется, пользователь в большинстве случаев готов отдать требуемую сумму, лишь бы вернуть свои данные.

Этот прием в настоящее время набирает все большую популярность. Следует отметить, что злоумышленники сейчас предпочитают шифровать данные не у какого-то домашнего пользователя (хотя такие случаи тоже нередки), а на корпоративных компьютерах и серверах — ведь домашний пользователь при всем желании не сможет заплатить столько же, сколько какая-нибудь даже небольшого размера фирма.

При возникновении подобной ситуации можно считать удачей, если злоумышленник требует перевести деньги банковским переводом — в этом случае его относительно легко вычислить (разумеется, обратившись своевременно в соответствующие органы). Но если в качестве платежных реквизитов указывается кошелек WebMoney, Яндекс.Деньги либо аналогичной интернет-системы, то здесь шансы обнаружить злоумышленника невелики. В данном случае хорошо, если после получения денег он не поленится выслать ключ для расшифровки данных.

Можно сказать, что удаленное шифрование данных является одним из самых неприятных и опасных видов интернет-мошенничества, которому подвержены незащищенные от вторжения извне компьютеры.

Каким же образом можно воспрепятствовать проникновению в свой компьютер удаленных злоумышленников? Одним из наиболее эффективных защитных средств является файрволл.

Файрволл (может называться также «брандмауэр» или «сетевой экран») — это своеобразный буфер, находящийся между локальным компьютером и Интернетом. Его смысл заключается в том, чтобы блокировать всяческие попытки проникновения как из Интернета в компьютер, так и из компьютера в Интернет различных программ, команд, заданий и т. д.

Может возникнуть вопрос: понятно, когда брандмауэр блокирует несанкционированный доступ из Интернета в компьютер, но зачем же блокировать выход из компьютера в Интернет? А затем, чтобы, например, троян либо иной шпион, проникший в компьютер до установки либо включения брандмауэра, не имел возможности выполнять полученное задание (рассылать спам с зараженного компьютера, отсылать информацию о компьютере и пользователе и т. п.). При этом разрешается выход в Интернет только тем приложениям, 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 имеется встроенный брандмауэр подключения к Интернету. Чтобы его включить, нужно в **Панели управления** выбрать категорию **Сеть и подключения к Интернету**, а затем — значок **Сетевые подключения**. В результате на экране откроется окно со списком имеющихся сетевых подключений. В данном окне нужно выделить курсором значок подключения, которое необходимо защитить брандмауэром, и в левой части окна в группе задач **Сетевые задачи** щелкнуть мышью на ссылке **Изменение настроек подключения** (рис. 1.1).

Рис. 1.1. *Переход к настройкам подключения*

После выполнения указанных действий на экране откроется окно просмотра и редактирования свойств текущего подключения. В данном окне следует перейти на вкладку **Дополнительно** (рис. 1.2).

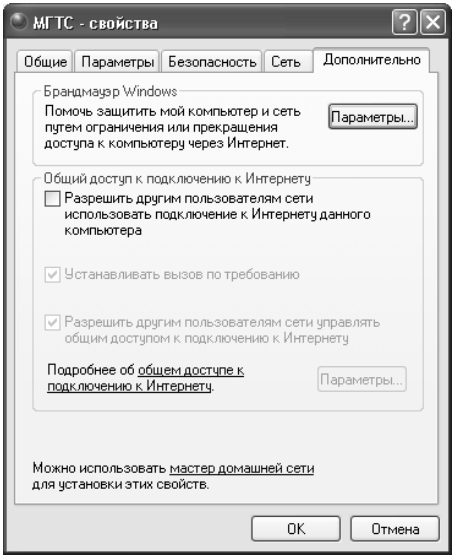

Рис. 1.2. *Редактирование свойств подключения*

На данной вкладке нужно нажать кнопку **Параметры**, и в открывшемся окне установить переключатель в положение **Включить (рекомендуется)** (рис. 1.3).

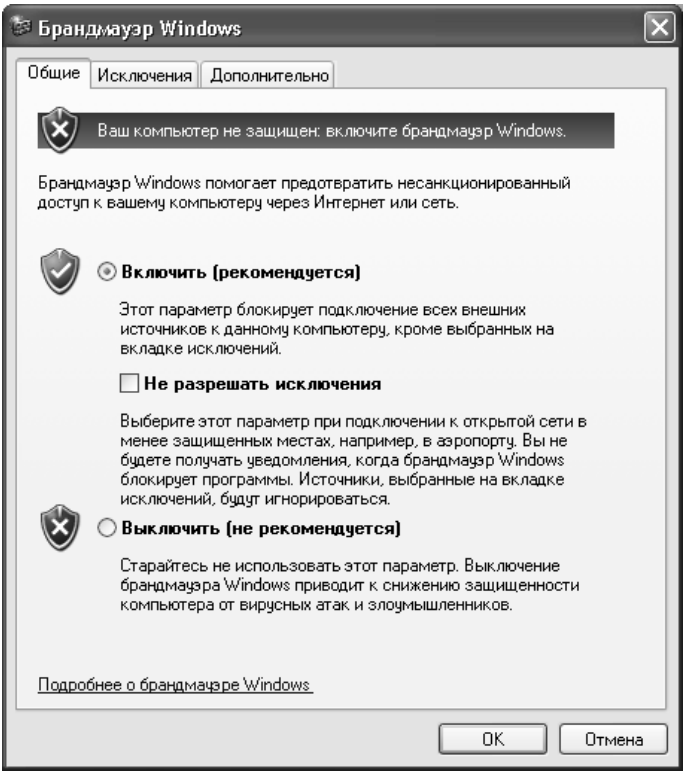

Рис. 1.3. *Включение брандмауэра Windows*

После выполнения указанных действий в каждом окне нажмите кнопку **ОК**.

Примечание. *По умолчанию брандмауэр Windows включен, и без особой надобности отключать его не рекомендуется.*

Кроме штатного брандмауэра Windows в настоящее время на рынке имеется достаточное количество сетевых экранов от сторонних разработчиков. Среди них можно порекомендовать защитный файрволл ZoneAlarm, являющийся сегодня одним из наиболее популярных и эффективных. Интерфейс программы представлен на рис. 1.4.

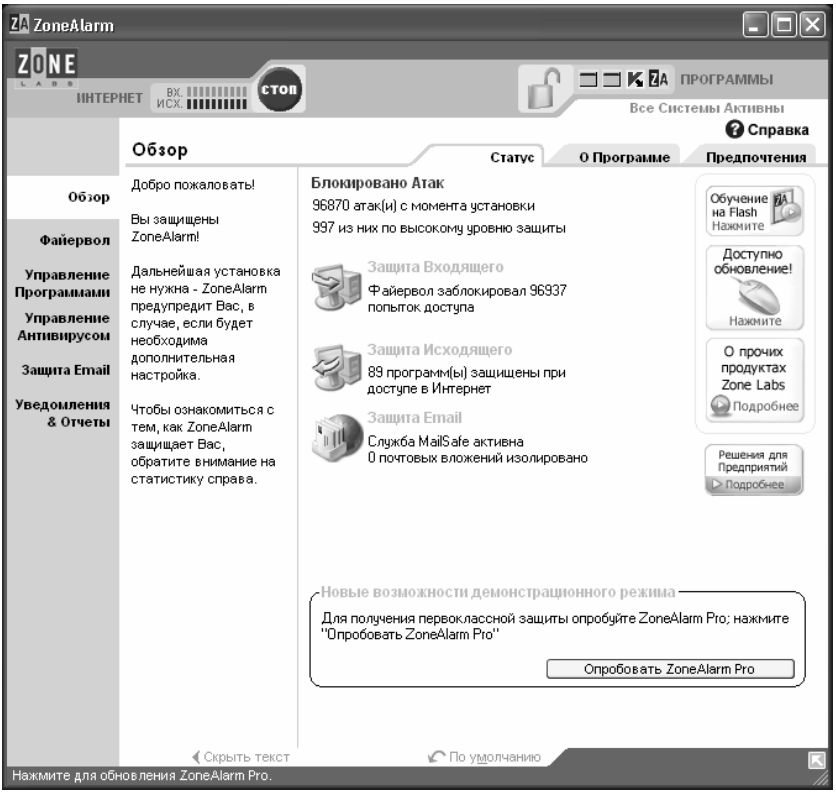

Рис. 1.4. *Защитная программа ZoneAlarm*

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 — ZoneAlarm не поддерживает русский язык (правда, в Интернете можно найти и скачать русификатор). В программе предусмотрена возможность тонкой настройки параметров защиты. В частности, пользователь самостоятельно указывает приложения, которым разрешен выход в Интернет (чаще всего это интернет-обозреватель, почтовая программа, ICQ и т. п.), определяет параметры доступа в компьютер извне. Попросту говоря, программа полностью контролирует входящий и исходящий трафик. Вы можете поместить программу в автозагрузку, включить режим скрытия своего IP-адреса и др.

Отметим, что файрволл ZoneAlarm в настоящее время является одним из самых надежных сетевых экранов.

Глава 2. ШТАТНЫЕ СРЕДСТВА WINDOWS, ПРЕДНАЗНАЧЕННЫЕ ДЛЯ ВОССТАНОВЛЕНИЯ ДАННЫХ

В некоторых случаях для восстановления данных можно воспользоваться штатными средствами Windows. В первую очередь это касается случаев, когда данные были ошибочно удалены в Корзину, а также — при нестабильной работе операционной системы или когда она вообще отказывается загружаться. В последних случаях можно попытаться запустить ее хотя бы один раз для того, чтобы успеть сохранить всю важную информацию на внешние носители или в Интернете перед полной переустановкой системы или другими кардинальными мерами (форматирование жесткого диска и т. п.), которые неминуемо приводят к потере всех хранящихся в компьютере данных.

2.1. Восстановление удаленных объектов из Корзины

В операционной системе Windows объекты (файлы и папки), которые были удалены с помощью клавиши **Delete**, **F8** или команды контекстного меню **Удалить** (в зависимости от того, где и как осуществлялось удаление), автоматически помещаются в **Корзину**. В данном случае **Корзина** представляет собой место для хранения ненужной информации (по аналогии с обыкновенной мусорной корзиной, имеющейся в каждом офисе).

При необходимости вы можете восстановить из **Корзины** помещенный в нее ранее объект. Как правило, эта операция осуществляется после ошибочного удаления данных.

Чтобы восстановить объект из **Корзины**, щелкните на нем правой кнопкой мыши и в открывшемся контекстном меню выполните команду **Восстановить** (рис. 2.1).

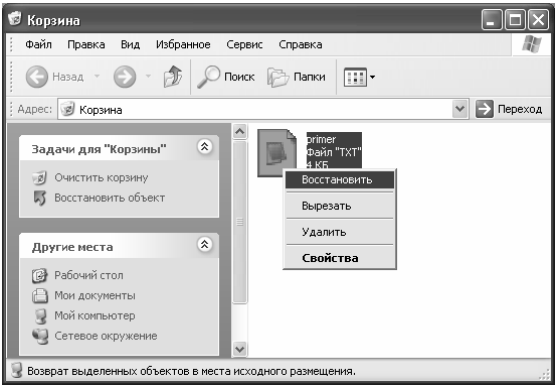

Рис. 2.1. *Восстановление объекта из* ***Корзины***

В результате объект будет восстановлен на том месте, откуда он ранее был удален, а из **Корзины** — исчезнет.

Стоит отметить, что периодически **Корзину** рекомендуется очищать от всего содержимого — чтобы не загромождать жесткий диск ненужной информацией. Это можно сделать двумя способами: щелкнуть правой кнопкой мыши на значке **Корзины** на рабочем столе и в открывшемся контекстном меню выбрать команду **Очистить корзину**, либо открыть **Корзину** и выполнить в ней команду главного меню **Файл ⇒ Очистить корзину**. Но учтите: в этом случае данные удаляются окончательно, и штатными средствами Windows вы их восстановить не сможете.

2.2. Загрузка последней удачной конфигурации системы

Иногда операционная система ведет себя совершенно непредсказуемо и нестабильно. О причинах подобных явлений мы говорили в предыдущей главе, а здесь расскажем о том, каким образом можно «оживить» ее хотя бы для спасения хранящейся в компьютере информации.

Приведенный здесь метод удобно использовать в случаях, когда система попросту отказывается загружаться, или после загрузки становится совершенно неработоспособной.

Включите компьютер или перезагрузите его с помощью кнопки **Reset**. Как только он начнет загружаться, нажмите и удерживайте клавишу **F8**. В результате через некоторое время на экране отобразится меню с вариантами загрузки. Как правило, в подобной ситуации нужно выбрать вариант загрузки последней удачной конфигурации (с работоспособными параметрами), но может потребоваться и что-то другое (например, загрузка системы в безопасном режиме).

Примечание. *Выбор требуемого варианта загрузки Windows осуществляется с помощью клавиш со стрелками*.

Если после выбора, например, варианта загрузки с последними работоспособными параметрами система успешно запустилась — не откладывая, сохраняйте всю важную информацию на внешние носители, в локальной сети либо в Интернете. Лишь после того как вы сохранили все данные, можно совершать какие-то попытки по реанимированию операционной системы (восстановление, переустановка полная или частичная, лечение и др.). Учтите: даже если в этот раз вам удалось удачно загрузить операционную систему — не факт, что это получится в следующий раз.

2.3. Восстановление системы из меню «Пуск»

В процессе эксплуатации системы могут возникать ситуации, когда нужно вернуться к одному из предыдущих ее состояний. Такая необходимость может быть обусловлена, например, нестабильной работой системы, неквалифицированным редактированием системного реестра, аппаратными сбоями и др. Функциональность восстановления системы позволяет «откатить» ее к стабильным параметрам работы, что нередко позволяет восстановить ее работоспособность хотя бы на время, достаточное для сохранения наиболее ценной информации.

Чтобы перейти в режим восстановления операционной системы, необходимо выполнить команду **Пуск ⇒ Все программы ⇒ Стандартные ⇒ Служебные ⇒ Восстановление системы**. При этом на экране откроется окно, изображенное на рис. 2.2.

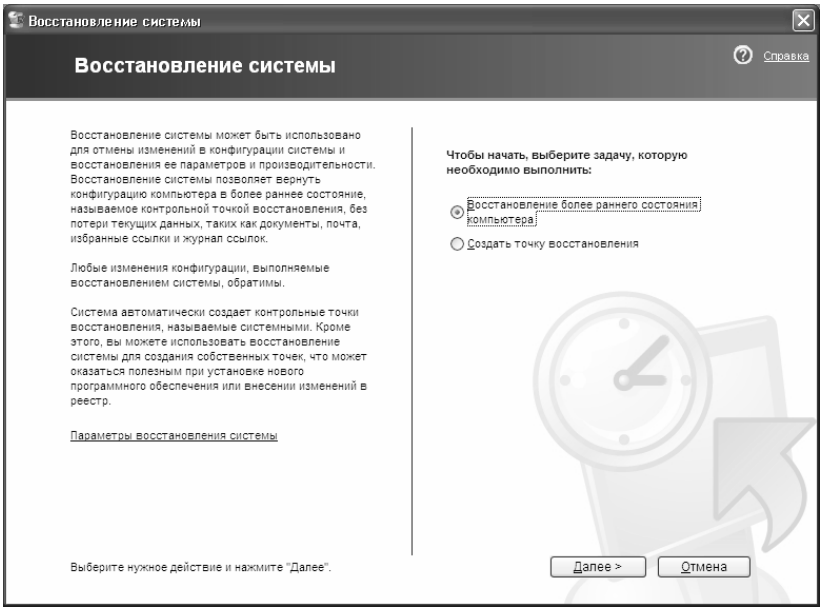

Рис. 2.2. *Восстановление операционной системы*

В данном окне с помощью переключателя необходимо выбрать одно из следующих действий:

- **Восстановление более раннего состояния компьютера**;
- **Создать точку восстановления**;
- **Отменить последнее восстановление** (доступно только после выполненного восстановления системы).

Конец ознакомительного фрагмента.
Приобрести книгу можно
в интернет-магазине
«Электронный универс»
e-Univers.ru