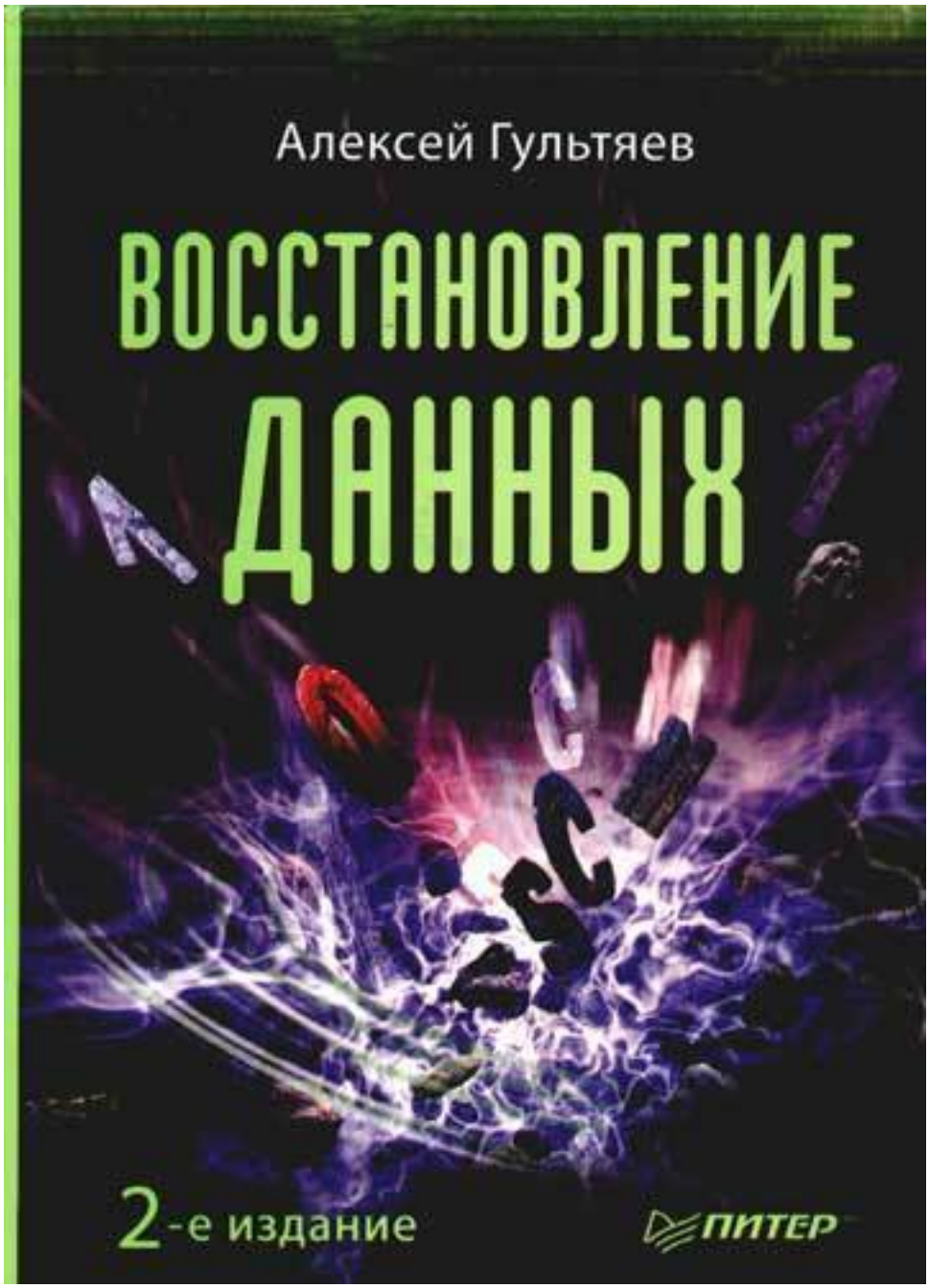

Алексей Гультяев
ВОССТАНОВЛЕНИЕ ДАННЫХ
2-е издание
ПИТЕР

Алексей Гультяев

Восстановление данных

«Питер»

Гультяев А. К.

Восстановление данных / А. К. Гультяев — «Питер»,

ISBN 5-469-01360-X

Чем более заметную роль начинает играть компьютер в нашей повседневной жизни, тем ценнее становится для нас хранящаяся в нем информация. Число различных факторов, угрожающих безопасности компьютерных данных, весьма велико. Здесь и вредоносные программы, и горе-специалисты, способные превратить своими советами ваш компьютер в бесполезный ящик, и, наконец, ваши собственные ошибки при работе с данными. Книга содержит полезные практические рекомендации, придерживаясь которых вы сможете не только избежать многих неприятностей в работе с компьютерной информацией, но и восстановить ее в случае потери.

ISBN 5-469-01360-X

Содержание

Алексей Гультяев
Восстановление данных

Введение

Чем более заметную роль играет компьютер в вашей повседневной жизни, тем ценнее становятся для вас хранящиеся в нем данные, и тем обиднее их потерять.

Вероятно, каждый владелец компьютера сталкивался с ситуацией, когда из компьютера бесследно исчезали только что созданные «непосильным трудом» документы или найденная на бескрайних просторах Интернета картинка. Возможно, читатель знаком и с такими случаями, когда компьютер вообще переставал загружаться, хотя только вчера вечером все было нормально. Все данные словно оказывались в сейфе с испорченным секретным замком. Отчего же такое происходит и можно ли с этим бороться?

Дело в том, что умный (с виду) компьютер пока еще не научился как следует сам себя защищать – себя и те данные, которые он хранит и обрабатывает. А защищаться есть от чего. Здесь и вредоносные программы, и горе-специалисты, способные превратить своими советами и неумелыми действиями ваш компьютер в бесполезный ящик, и внезапные отключения электричества, и, наконец, ваши собственные ошибки в работе.

Таким образом, первый шаг в деле восстановления данных – это их защита, то есть предотвращение потери имеющейся информации. Именно по названной причине первые две главы книги посвящены вопросам, связанным с повышением безопасности данных, с которыми вы работаете. Приведенный в них материал должен помочь выбрать наиболее подходящие для вас (точнее – для вашего компьютера) средства и методы защиты от разных неприятных неожиданностей. Причем совершенно не обязательно устанавливать на компьютер именно те программы, которые описаны в книге. Главное – осознать необходимость присутствия на компьютере «защитных» программных средств и приучаться регулярно и правильно их использовать.

Третья глава – «Настройка системных параметров» – посвящена прежде всего правильному (опять-таки с точки зрения безопасности) размещению данных на жестких дисках компьютера. Наличие этой главы обусловлено тем, что основным хранителем данных по-прежнему остается винчестер. Выход из строя или неправильное использование именно этого устройства способны сделать владельца компьютера глубоко несчастным человеком. Чтобы ваши действия были уверенными, а их результат – предсказуемым, здесь же рассмотрены основные особенности файловых систем FAT32 и NTFS.

Глава 4 полностью посвящена резервному копированию данных – наиболее простому и надежному способу обеспечения их сохранности. И, к тому же, наиболее универсальному: с его помощью можно одинаково успешно восстанавливать как системные компоненты, так и данные пользователя.

Главы 5 и 6 называются, соответственно, «Восстановление системной информации» и «Восстановление данных пользователя». Почему именно в таком порядке? Казалось бы, учиться лучше на менее «взрывоопасных» ситуациях. Однако в результате изучения материала пятой главы вы должны уяснить, что восстановление удаленных или испорченных системных данных – вполне реальная задача. Достаточно лишь соблюдать хладнокровие и аккуратность, а также придерживаться некоторых не очень сложных правил. Тем более что в вашем распоряжении предостаточно соответствующих инструментов. И наконец, последний аргумент: если ничто не помогает, систему можно переустановить. Повторная ее настройка займет значительно меньше времени, нежели повторное создание документов, мультимедийных файлов и других данных, о восстановлении которых рассказано в шестой главе. В этой же главе значи-

тельное внимание уделено восстановлению данных на сменных носителях – компакт-дисках, DVD, картах памяти.

Завершает книгу глава «Восстановление данных на жестких дисках». В ней рассмотрены ситуации, когда по тем или иным причинам автоматические средства восстановления оказываются бессильны, и человеку приходится действовать «голыми руками», погружая их по локоть в двоичные нули и единицы, разбросанные по жесткому диску. Еще лет десять назад такая глава занимала бы центральное место в книге под названием «Восстановление данных». Однако поскольку сейчас существуют эффективные средства автоматического восстановления и программы резервного копирования, изложенные в этой главе методы можно отнести, скорее, к разряду экстремальных. И предназначены они в первую очередь для любителей острых ощущений и тех, кто никак не может заставить себя применять «цивилизованные» методы защиты своих данных.

От издательства

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

Мы будем рады узнать ваше мнение!

Подробную информацию о наших книгах вы найдете на веб-сайте издательства http://www.piter.com.

Глава 1
Что имеем – не храним, или Почему теряются данные

Потерять можно все – любые данные, практически на любом носителе: на жестких дисках компьютера, на гибком диске, а также файлы на компакт-диске или на флэш-карте. Более того, пострадать может даже программа BIOS, хранящаяся в постоянном запоминающем устройстве материнской платы. Разумеется, последствия потери различных данных могут быть разными. Одно дело – лишиться текстового файла из пяти строчек, и совсем другое – когда портится системный реестр.

Не торопитесь восстанавливать

В каждом из таких случаев следует использовать адекватные средства и методы восстановления данных. Например, небольшой текстовый файл можно просто набрать заново, а для восстановления системного реестра может потребоваться полная переустановка операционной системы.

Поэтому, прежде чем приступать к процедуре восстановления, полезно ответить на следующие вопросы:

данные какого типа вы потеряли;

на каком носителе (запоминающем устройстве) размещались данные;

каким образом были созданы (получены) утраченные данные;

что явилось причиной утраты (или повреждения) данных.

Имея ответы на приведенные вопросы, вы можете сберечь не только собственное время, но и изрядное количество своих нервных клеток.

Например, удалив случайно рисунок, скачанный из Интернета, совсем не обязательно пытаться восстановить его с помощью специальных программ. Проще скачать его еще раз. Причем, скорее всего, подключаться к Интернету не потребуется, поскольку файл остался в кэше вашего веб-браузера.

А бывает и так, что тревога оказывается ложной. Например, открыв в поисках нужного файла некоторую папку и не обнаружив его там, вы можете решить, что файл был по какой-то причине удален. А он, родимый, жив-здоров и сидит себе на месте, но в другой папке. Это случается, когда в используемой вами программе установлены параметры сохранения файлов по умолчанию. Скажем, редактор MS Word очень часто пытается сохранить новый документ в папке Мои документы. Однако на компьютере может оказаться несколько папок с таким именем (рис. 1.1). И если вы работаете с одной из этих папок, а MS Word – с другой, то созданный документ можно «потерять».

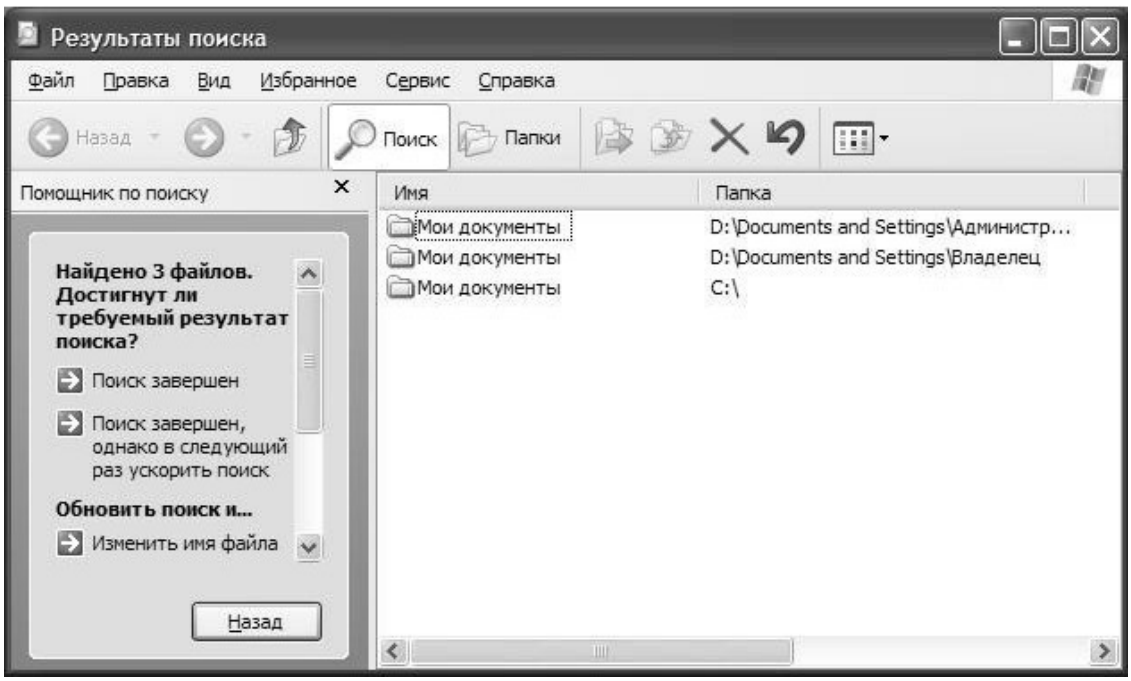


Рис. 1.1. Файл может «потеряться» в одноименных папках

Теперь вернемся к первому из поставленных ранее вопросов: данные какого рода могут быть потеряны?

В самом общем случае все «теряемые» данные можно разделить на три вида:

пользовательские файлы и папки;

прикладные программы, установленные пользователем на компьютере;

системные файлы (в том числе исполняемые, с расширениями. exe,bat,com) и папки.

Чем различаются перечисленные виды данных? Различий много. Однако, с точки зрения восстановления данных, основное из них состоит в следующем. Для восстановления системных файлов и папок предусмотрены специальные средства, входящие в состав операционной системы, в то время как о восстановлении своих файлов владелец компьютера должен заботиться сам. Например, регулярно создавая их резервные копии.

ПРИМЕЧАНИЕ _____

Несколько забегая вперед, следует сказать, что резервное копирование – это вообще универсальное «лекарство» практически от всех проблем, связанных с потерей данных. В силу важности вопросов, связанных с резервным копированием, они будут подробно рассмотрены в отдельной главе.

Чтобы восстановить работоспособность прикладной программы, бывает недостаточно заменить файлы их резервными копиями. Часто приходится дополнительно восстанавливать и/или редактировать системный реестр и другую системную информацию.

Что касается второй характеристики потерянных данных (типа носителя), то она оказывает большое влияние на выбор методов и для защиты данных, и для их восстановления. При этом именно учет типа носителя требует наличия дополнительных знаний, которые в повседневной работе на компьютере вовсе и не нужны. Например, чтобы восстановить данные на жестком диске, иногда требуется знать тип используемой файловой системы, способ адресации физического пространства диска, размещение и формат служебных зон и многое другое. Соответственно, при более глубоком анализе причин «исчезновения» того или иного файла может оказаться, что как раз с файлом ничего не случилось, а повреждена служебная информация файловой системы.

Если же речь идет о компакт-диске, то «реаниматор» должен, по крайней мере, знать, к какому типу относится CD с данными: «только для чтения» (CD-ROM), записываемый (CD-R) или перезаписываемый (CD-RW). Кроме того, вероятность успешного восстановления существенно возрастет, если вы имеете представление об особенностях логических форматов записи на компакт-диски и DVD.

ПРИМЕЧАНИЕ

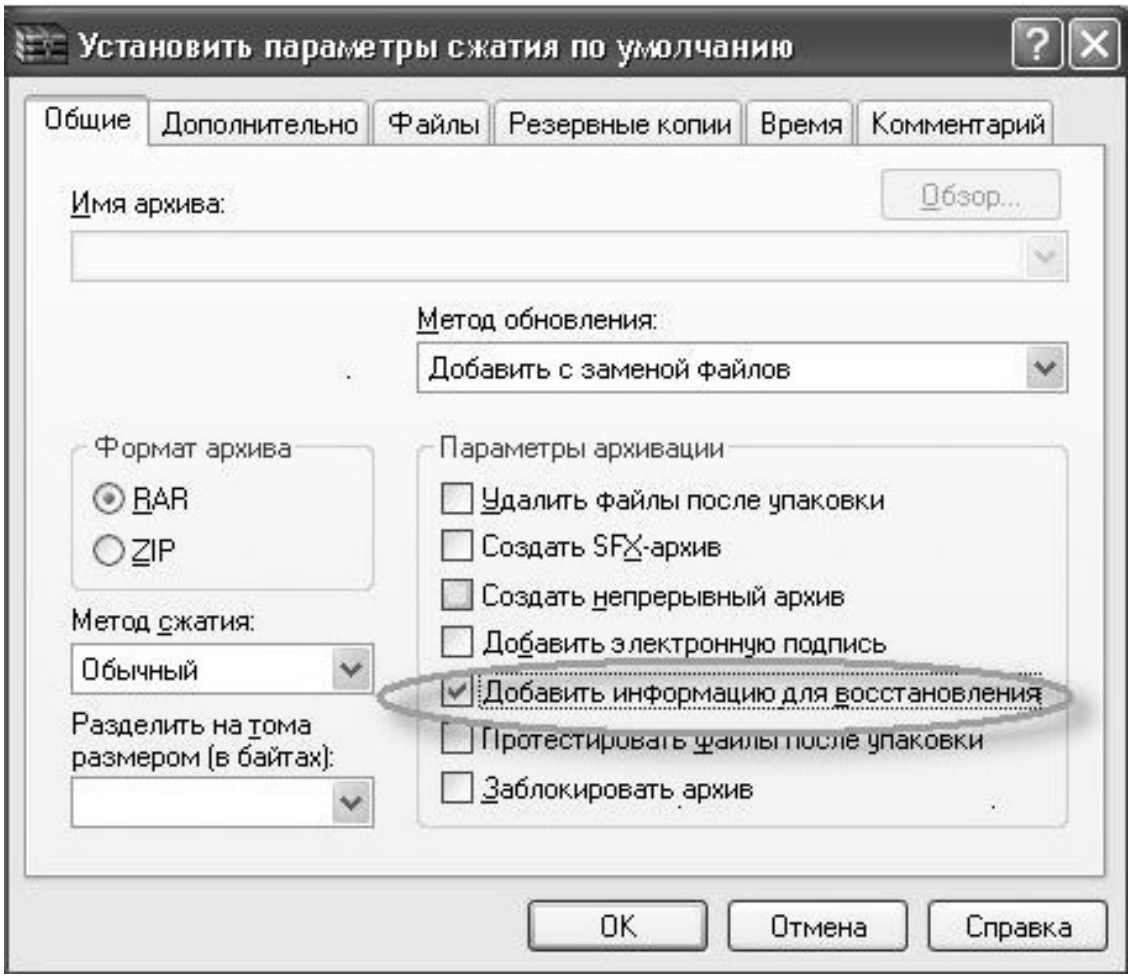
Сделанная выше оговорка относительно того, что неплохо бы знать тип и формат записи поврежденного носителя CD/DVD, – это вовсе не шутка. Практика показывает, что далеко не все пользователи представляют себе, как именно хранятся данные на таких носителях.

Программное средство, с помощью которого был создан (записан) файл, также имеет немаловажное значение. Дело в том, что некоторые «особо умные» программы способны в критических ситуациях автоматически создавать резервную копию данных, с которыми работает пользователь, и затем восстанавливать их. Например, такую способность иногда проявляет MS Word; более стабильны в этом отношении веб-браузер Opera и HTML-редактор Macromedia HomeSite 5. Собственной «службой спасения» располагает также популярный

архиватор WinRAR. Это и понятно: порча одного архивного файла может означать потерю нескольких папок с файлами, упакованных в архив (рис. 1.2).

СОВЕТ _____

Если программа предоставляет возможность восстановления данных, то ею следует воспользоваться.



Причины, по которым данные могут быть утрачены, заслуживают отдельного обсуждения. Им посвящен следующий раздел.

Виды угроз безопасности информации

Специалисты в области безопасности информации считают, что компьютерные данные подвержены трем типам опасностей, к которым относятся:

нарушение конфиденциальности – данные становятся известны тому, кто их знать не должен;

нарушение целостности – данные частично или полностью изменяются (модифицируются) вопреки желанию их владельца; например, нарушением целостности является изменение форматирования документа или изменение логических связей между элементами базы данных;

нарушение доступности – владелец компьютера лишается возможности работать с данными вследствие отказа сервисов, функций или служб, предназначенных для их обработки; например, если возникают проблемы с идентификацией на почтовом сервере, вы не сможете прочитать поступившие электронные письма, даже если они не повреждены.

В свою очередь, опасность каждого типа может быть связана как со случайными факторами, так и с преднамеренными действиями злоумышленников. Опасности первого рода называют *случайными угрозами,* а опасности второго рода – *умышленными угрозами.*

В государственных и коммерческих учреждениях и организациях наиболее тяжелые последствия связаны с успешно осуществленными умышленными угрозами. Объясняется это тем, что в таких случаях происходит целенаправленное воздействие на уязвимые точки системы защиты информации.

Для владельцев домашних компьютеров вероятность умышленных угроз мала: вряд ли кто-нибудь из них станет утверждать, что за его файлами охотятся агенты спецслужб или конкуренты из соседнего подъезда. Поэтому основные мероприятия по защите «домашних» данных должны быть направлены как раз на предотвращение случайных угроз и на преодоление их последствий.

Тем не менее истинность поговорки «предупрежден – значит вооружен» проверена жизнью, а потому для начала рассмотрим умышленные угрозы.

Умышленные угрозы

Итак, умышленных угроз следует опасаться лишь тому, кто считает, что у него есть враги (недоброжелатели), недобросовестные конкуренты или друзья, способные на соответствующие «шутки».

Теоретически, перечисленные выше лица могут использовать для реализации своих недобрых намерений самые разнообразные средства: перехват побочных электромагнитных излучений, визуальное наблюдение, ведение агентурной работы, перехват телефонных переговоров, применение радиозакладок и даже поджог (с целью уничтожения компьютерных данных вместе с самим компьютером). Однако для большинства владельцев ПК наиболее реальной угрозой представляется так называемый *несанкционированный доступ к информации* (сокращенно – НСД).

ПРИМЕЧАНИЕ _____

Вопреки достаточно распространенному мнению, НСД не является синонимом любого «неразрешенного» доступа к данным. В частности, «подсматривание» или «подслушивание» с помощью специальных технических устройств и даже перехват электромагнитного излучения – это не НСД. Согласно документам Государственной технической

комиссии (основного государственного ведомства, занимающегося вопросами безопасности компьютерной информации), НСД предполагает неправомерный доступ к информации с помощью штатных средств вычислительной техники. То есть, например, удаление «чужого» файла штатными средствами Windows – это НСД, а похищение жесткого диска – это не НСД.

Несмотря на наличие регламентированного определения НСД, это достаточно широкое понятие. По той причине, что даже штатные средства компьютера предоставляют злоумышленникам массу способов для нарушения конфиденциальности, целостности и доступности данных. Например, злоумышленник может войти в систему под вашим паролем и скопировать текст дипломной работы или изменить авторство созданного вами документа.

С распространением сетевых технологий все большая опасность для персональных данных исходит извне, то есть со стороны других пользователей Сети. Самый, пожалуй, «популярный» на сегодня вариант злонамеренного воздействия на чужие данные – это внедрение в систему того или иного вредоносного программногообеспечения. А наиболее простой и распространенный способ внедрения – это почтовое отправление (электронное, разумеется).

Поскольку вредоносному программному обеспечению посвящен специальный раздел этой главы, сейчас мы обратимся к другим видам угроз, которые возможны при работе в Сети:

несанкционированный доступ к сетевым ресурсам; например, злоумышленник может воспользоваться принтером, подключенным к компьютеру, работающему в сети (он вряд ли захочет затем забрать распечатку, но объем выводимых данных может привести к исчерпанию картриджа или блокированию принтера);

раскрытие и модификация данных и программ, их копирование; например, злоумышленник может, получив доступ к жесткому диску компьютера, отыскать на нем сетевое имя и пароль пользователя, под которым тот подключается к Интернету;

раскрытие, модификация или подмена трафика вычислительной сети; характерный пример – «бомбардировка» почтового сервера фиктивными письмами, что способно привести к перегрузке сервера;

фальсификация сообщений, отказ от факта получения информации или изменение времени ее приема; например, недобросовестный диспетчер может аннулировать заявку на проведение ремонтных работ или изменить время ее приема, чтобы «спихнуть» заявку на своего сменщика;

перехват и ознакомление с информацией, передаваемой по каналам связи; скажем, если вы решите заказать через Интернет железнодорожные билеты с доставкой на дом, то злоумышленники вполне могут узнать и адрес, и период времени, в течение которого хозяева будут в отъезде.

Очевидно, что приведенный перечень угроз не является исчерпывающим, однако он вполне достаточен для подтверждения того, что при отсутствии должной защиты ваши данные уязвимы.

Кстати, *уязвимость*– это еще одно важное понятие в теории (и в практике) защиты информации. Под уязвимостью понимают такое свойство системы, которое позволяет реализовать соответствующую угрозу. Например, система, не содержащая в своем составе средств антивирусного контроля, уязвима по отношению к вирусам; система, в которой вход пользователей осуществляется без использования паролей, уязвима с точки зрения несанкционированного доступа.

Случайные угрозы

«Все, что может случиться, – случается; что не может случиться, – случается тоже», – гласит известный закон Мэрфи.

На самом деле основная причина всех неприятных случайностей – это недостаточно бережное отношение владельца к компьютеру вообще и к компьютерным данным в частности. Иначе говоря, недостаточный уровень «компьютерной грамотности».

В частности, многие новички полагают, что нет никакой принципиальной разницы между компьютером и другой бытовой техникой, например холодильником, стиральной машиной или DVD-плеером. А разница есть.

Первое отличие состоит в том, что у владельца компьютера имеются практически неограниченные возможности по управлению его работой. Вы можете устанавливать, убирать или заменять внешние устройства и электронные компоненты, вплоть до «сердца» и «мозга» – процессора и оперативной памяти, устанавливать и удалять или изменять программное обеспечение, в том числе «душу» компьютера – операционную систему. Можно ли проделать то же самое с холодильником или телевизором?

Второе отличие, еще более важное, заключается в том, что с помощью компьютера вы можете творить – создавать то, чего до вас не создавал никто. В том числе и программы, поведение которых оказывается неподвластным их создателю. Вот, например, отрывок из письма читателя в один популярный компьютерный журнал: «Уважаемая редакция, недавно написал программу-перекодировщик текстовых файлов. По размеру программа совсем небольшая, однако после запуска и нескольких минут работы на экране появляется сообщение: „Недостаточно ресурсов для завершения операции". После этого система зависает…».

Вследствие указанных причин на каждом отдельно взятом компьютере может быть создана такая комбинация аппаратно-программных средств, которую не в состоянии предсказать ни один компьютерный гуру, включая производителей «железа», программного обеспечения и сотрудников служб технической поддержки. Зачастую оказывается очень сложно прогнозировать поведение конкретного компьютера в той или иной ситуации.

> ПРИМЕЧАНИЕ
>
> Именно поэтому, обращаясь за помощью к специалистам, постарайтесь как можно точнее описать конфигурацию аппаратно-программных средств компьютера и перечень тех действий, которые выполнялись непосредственно перед возникновением сбоя или отказа системы.

> **СОВЕТ _____**
>
> Для восстановления работоспособного состояния системымогут оказаться полезны сведения, занесенные работающей программой в файл протокола (или в журнал). Обычно такие файлыимеют расширение. log и содержат записи в обычном текстовом формате. Поэтому, если новая программа, устанавливаемая вами на компьютер, предлагает вести файл протокола, не отказывайтесь от этого предложения.

Иногда причиной неприятностей становится излишняя самоуверенность. Некоторые владельцы компьютеров без тени сомнений настраивают «под себя» критически важные параметры системы, отключают Корзину, не читают сообщения, выводимые системой на экран и, разумеется, не утруждают себя созданием резервных копий даже самых ценных данных.

Имеются, конечно, и другие причины неприятных сюрпризов, не зависящие от уровня подготовки и характера владельца ПК: внезапные отключения электричества или, что еще хуже, скачки напряжения; отказы и сбои оборудования, неожиданные проявления ошибок в, казалось бы, надежных программах; чисто «механические» казусы, когда, например, щелкают на кнопке Нет вместо кнопки Да.

> ПРИМЕЧАНИЕ

Абсолютно «надежных» программ (то есть программ без ошибок) не бывает. Объясняется это тем, что разработчики при всем желании не могут проверить (протестировать) работоспособность создаваемой программы для всех возможных сочетаний входных данных, конфигураций взаимодействующих программ и действий пользователей. Поэтому рано или поздно программа «натыкается» на одну из таких непроверенных ситуаций, и (по упомянутому выше закону Мэрфи) именно в этой ситуации проявляется допущенная ошибка. Иногда ошибка оказывается фатальной и приводит к потере данных или к отказу всей системы. Ясно, что разработчики программы не имели злого умысла, но…

В роли «без вины виноватого» может оказаться и ваш друг, предложивший переписать интересующий вас файл с зараженного вирусом гибкого диска (сам предварительно не проверил, а вы не подстраховались…).

Итак, перечислим наиболее вероятные угрозы случайного характера:

ошибки обслуживающего персонала и пользователей;

потеря информации, обусловленная неправильным хранением данных;

случайное уничтожение или изменение данных;

сбои и отказы аппаратной части компьютера;

перебои электропитания;

некорректная работа программного обеспечения;

непреднамеренное заражение системы компьютерными вирусами или другими видами вредоносного программного обеспечения.

ВНИМАНИЕ

Хотя вредоносные программы и оказались в приведенном перечне на последнем месте, по своей «вредности» они опережают многие другие угрозы безопасности данных.

Разновидности вредоносного программного обеспечения

Как ни странно, до сих пор нет единой классификации известных видов вредоносных программ. Вот одна из причин тому: в последнее время все больше появляется универсальных «вредителей», объединяющих в себе наиболее гнусные качества.

«Вирусами» следует называть только такие вредоносные программы, которые способны к *саморазмножению.* Что понимается под этим свойством? Способность вируса создавать собственную копию и внедрять ее в тело заражаемого файла или в системную область (загрузочный сектор) диска.

Помимо вирусов существуют еще так называемые *программные закладки* – программы или отдельные модули программ, которые выполняют скрытые функции, способные нарушить конфиденциальность, доступность или целостность данных. Программные закладки, в свою очередь, разделяются на два вида: программы-шпионы (spyware) и логические бомбы. Программа-шпион выполняет свои функции в течение всего периода пребывания на компьютере пользователя. Логическая бомба срабатывает один раз (по внешнему сигналу или по своим «внутренним часам»).

Иногда к «шпионским» относят также программы, получившие обобщенное наименование AdWare. Приложения такого типа содержат дополнительный код, который обеспечивает вывод на экран дополнительных («всплывающих») окон, содержащих информацию рекламного характера. Кроме того, некоторые подобные программы отслеживают личную информацию пользователя (возраст, пол, посещаемые веб-сайты, адреса электронной почты) и передают ее своим «хозяевам».

Третий вид вредоносных программ – это почтовые черви (mail worms). Червь представляет собой разновидность вируса, который распространяется вместе с вложением к электронному письму и (за редким исключением) не наносит вреда локальным данным. Механизм распространения вируса-червя в сети основан на том, что он отыскивает на компьютере адреса электронной почты и рассылает себя по этим адресам. Наиболее «продвинутые» черви способны генерировать текст отправляемого письма и наименование темы (тело червя прикрепляется к письму в виде вложения).

Рассмотрим названные виды вредоносных программ подробнее.

Компьютерные вирусы

В общем случае жизненный цикл компьютерного вируса содержит следующие этапы:

внедрение (инфицирование);

инкубационный период, в течение которого вирус себя не проявляет (как правило, ожидает либо появления подходящего объекта для заражения, либо выполнения заданных автором вируса условий);

саморазмножение (может выполняться различными способами, о которых будет сказано ниже);

выполнение специальных функций, то есть собственно выполнение тех вредных действий, для которых вирус создавался;

проявление – заключается в демонстрации вирусом своего присутствия на компьютере (обычно в визуальной или в звуковой форме).

Перечисленные этапы не являются обязательными (за исключением этапов инфицирования и саморазмножения) и могут иметь иную последовательность. Например, вирус может сначала сообщить о своем присутствии и лишь после этого заняться заражением. Особую опас-

ность представляет этап выполнения специальных функций, которые могут привести к катастрофическим последствиям.

Как уже было сказано выше, любая классификация вирусов достаточно условна. Тем не менее один из вариантов классификации мы все-таки приведем.

В соответствии с ним вирусы подразделяются на классы по следующим признакам:

среда обитания;

способ заражения;

деструктивная возможность;

особенности алгоритма вируса.

По **среде обитания** компьютерные вирусы можно разделить на загрузочные, дисковые, файловые, флэш-вирусы и сетевые.

Загрузочные вирусы внедряются в загрузочный сектор диска (boot-сектор) или в сектор, содержащий системный загрузчик винчестера.

Дисковые вирусы замечательны тем, что способны работать с физическими секторами жестких дисков. Такой вирус захватывает свободные (или даже занятые данными) секторы диска, устанавливает для них в файловой системе признак «плохих» (такие секторы в дальнейшем не распределяются под данные) или «специальных» (не подлежащих перезаписи) и «живет» в них до прихода доктора-антивируса.

К *файловым* относят вирусы, заражающие исполняемые файлы (файлы с расширениями. exe,com,bat). Особой разновидностью файловых вирусов являются так называемые *макровирусы.* Они «живут» в макросах – программах, написанных на языке VBA (Visual Basic Application), которые используются для расширения функциональных возможностей приложений из комплекта MS Office.

Еще один, наиболее «современный» тип файловых вирусов – это вредоносные сценарии (скрипты), написанные на одном из популярных скриптовых языков программирования (VBScript или JavaScript) и входящие в состав HTML-страниц. Для краткости будем именовать такие вирусы *сценарными* (или скриптовыми).

Флэш-вирусы обязаны своим названием микросхемам перезаписываемой энергонезависимой памяти (флэш-памяти). Как известно, в современных компьютерах такие микросхемы используются на материнских платах для хранения кода программы BIOS. Неудивительно, что компьютеры, «подцепившие» флэш-вирус, зачастую вообще оказываются неспособны загружаться.

Сетевые вирусы для распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Помимо перечисленных, существуют и «комбинированные» вирусы – например, файлово-загрузочные, способные заражать как файлы, так и загрузочные секторы дисков. Такие вирусы, как правило, работают по довольно сложным алгоритмам и часто применяют оригинальные методы проникновения в систему.

> ПРИМЕЧАНИЕ
>
> По состоянию на ноябрь 2005 года почтовые и сетевые черви составляли около 78 % от всех выявленных вирусов, файловые вирусы – около 20 %, загрузочные и другие вирусы в общей сложности составляют около 2 % (по данным Лаборатории Касперского).

По **способу заражения** вирусы подразделяются на резидентные и нерезидентные.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти (ОП) свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них. Обычно эта процедура предусматривает проверку, не присутствует ли уже в объекте копия вируса. Если объект «чист», то вирус копируется из памяти в заражаемый объект с модификацией его первой команды. Объектами заражения в этом случае могут быть исполняемые программы на жестком диске и на гибких дисках. Резидентные вирусы находятся в памяти и активны вплоть до выключения или перезагрузки компьютера. Резидентными можно считать макровирусы, поскольку они постоянно присутствуют в памяти компьютера в течение всего времени работы приложения, использующего «вредоносный» макрос. Соответственно, все документы, созданные или просто открытые в это время, будут заражены.

Нерезидентные (транзитные) вирусы не заражают ОП и активны ограниченное время. Транзитные вирусы не остаются в памяти после выполнения зараженной программы. Такой вирус перед передачей управления исходной программе ищет незараженный файл, пригодный для внедрения.

По **деструктивным способностям** вирусы можно разделить на:

безвредные;

неопасные;

опасные;

очень опасные.

Безвредные вирусы только уменьшают объем свободной памяти на диске в результате своего распространения.

Влияние *неопасных* вирусов ограничивается также уменьшением свободной памяти на диске и дополнительно сопровождается графическими, звуковыми и другими эффектами.

Опасные вирусы приводят к серьезным сбоям в работе компьютера.

В результате работы *очень опасных* вирусов уничтожаются программы, данные, удаляется необходимая для работы информация, записанная в системных областях памяти. Особо опасны вирусы, прикрепляемые к объектной библиотеке какого-либо компилятора. Такие вирусы автоматически внедряются в любую программу, работающую с инфицированной библиотекой. Известны также вирусы, способные разрушать BIOS компьютера, что приводит к невозможности его загрузки.

Вообще известные в настоящее время вирусы могут выполнять следующие разрушительные функции:

изменение данных в файлах;

изменение данных, передаваемых через параллельные и последовательные порты;

изменение назначенного диска (запись информации производится не на диск, указанный пользователем, а на диск, указанный вирусом);

переименование файлов;

форматирование отдельных частей жесткого диска (гибкого диска) или даже всего диска;

уничтожение, изменение или перемещение загрузочного сектора диска;

снижение производительности системы из-за постоянного выполнения паразитных программ;

отказ в выполнении определенной функции (например, блокировку клавиатуры, блокировку загрузки программы с защищенного от записи гибкого диска и т. д.).

Вирусы могут использовать следующие алгоритмы работы:

стелс-алгоритмы;

самошифрование и полиморфизм;

нестандартные приемы.

Применение *стелс-алгоритмов* (от англ. stealth – «невидимка») позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение-запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. В случае макровирусов наиболее популярный способ – запрет вызовов меню просмотра макросов. Один из первых файловых стелс-вирусов – вирус «Frodo», первый загрузочный стелс-вирус – «Brain».

Самошифрование и *полиморфизм* (от англ. polymorphism – «многообразие») используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру обнаружения вируса. Полиморфик-вирусы – это вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Различные *нестандартные приемы* часто используются в вирусах для того, чтобы как можно глубже спрятать себя в ядре ОС (как это делает вирус «ЗАРАЗА»), защитить от обнаружения свою резидентную копию (вирусы «TPVO», «Trout2»), затруднить лечение от вируса (например, поместив свою копию в Flash-BIOS) и т. д.

Программы-шпионы

Почему из программных закладок уделено внимание только программам-шпионам? Дело в том, что логические бомбы – вещь достаточно сложная и дорогостоящая, и потому на уровне «домашних» компьютеров практически не встречаются. Можно привести такой пример использования логических бомб. В свое время (в начале 90-х годов прошлого века) для вооруженных сил Ирака были закуплены во Франции зенитно-ракетные комплексы. Как потом стало известно, их программное обеспечение содержало логические бомбы. Когда США начали боевые действия против Ирака (операция «Буря в пустыне»), логические бомбы были активизированы по сигналам с военных спутников. В результате практически вся система противовоздушной обороны Ирака оказалась выведенной из строя.

Но вернемся к более «мирным» программам-шпионам. На такие программы обычно возлагаются следующие функции:

сбор сведений о программном обеспечении, установленном на компьютере (в том числе тип и версия используемой операционной системы);

перехват клавиатурного ввода (в частности, отслеживание вводимых паролей, сетевых имен и т. д.);

поиск на жестком диске (дисках) персональных данных;

выявление адресов посещаемых веб-сайтов, адресов электронной почты и т. п.;

создание снимков экрана или окон конкретных активных приложений (некоторые «шпионы» способны также записывать целые видеоклипы о работе владельца компьютера).

Большинство программ-шпионов умеет передавать собранные сведения своему «хозяину», то есть лицу (или организации), заславшему «шпиона».

Наиболее простой и распространенный на сегодняшний день способ передачи «шпионом» собранных сведений – это пересылка их посредством Интернета (например, по электронной почте).

Кому могут принести пользу собранные сведения? В первую очередь на ум приходят пресловутые спецслужбы, контролирующие личную жизнь граждан. Но это, скорее, исключение. Значительно большую заинтересованность в сборе сведений о конфигурации компьютера «рядового» пользователя проявляют производители программного обеспечения и аппаратных компонентов вычислительной техники. Конкретные цели сбора сведений могут быть разными:

это и борьба с пиратским использованием программ, и исследование потребительского рынка, и конкурентная борьба, а также другие смежные направления.

ПРИМЕЧАНИЕ

Иногда программы-шпионыиспользуются не для нападения, а для защиты – когда владелец компьютера устанавливает такую программу сам, чтобыона следила за работой на компьютере других лиц. Частный случай подобного применения «шпионов» – контроль за действия подчиненных со стороны руководства.

Теперь о том, каким образом программы-шпионы попадают на компьютер. Может применяться тот же способ, что и при заражении вирусами, то есть «шпион» может «прятаться» внутри файла данных или исполняемого файла. Однако это не самый популярный вариант, поскольку размер «шпиона» обычно значительно больше размера вируса, и спрятать его внутри файла-контейнера непросто.

Значительно чаще «шпион» входит в дистрибутив какой-либо безобидной (или даже полезной) программы, приобретаемой или скачиваемой из Интернета. В процессе установки такой программы на компьютер параллельно производится также установка «шпиона». Нередко «шпион» прописывается на компьютере по всем правилам: с регистрацией в системном реестре, с созданием собственной папки, собственных типов файлов данных и т. д. Благодаря этому «шпион» зачастую продолжает «жить и работать» даже после удаления той основной программы, в которой он был спрятан.

Таким образом, программа, обеспечивающая установку «шпиона» на компьютер, играет роль своеобразного троянского коня, в недрах которого прячется неприятный сюрприз.

ПРИМЕЧАНИЕ

Изначально именно программы, содержащие недекларированные возможности, получили прозвище «троянские кони», или, в сокращенном варианте, «троянцы» (ато и вовсе «трояны»). Однако со временем входившая в них шпионская начинка стала использоваться самостоятельно (или кочевала из одной программы-контейнера в другую). В результате наименование «троянец» стало применяться не к контейнеру, а собственно к вредоносной программе. Сейчас можно встретить программы-вирусы, которые называют троянцами, хотя они используют отнюдь не «троянскую» технологию распространения (например, TROJ_EVIL, распространяющийся как файловый вирус). Имя вируса, данное ему автором, далеко не всегда соответствует типу вируса. Например, если вирус называется Worm, это еще не значит, что перед вами действительно вирус-червь. Возможно, его создателю просто понравилось это словечко.

На сегодняшний день известно несколько достаточно популярных программ, содержащих в своем составе шпионские модули, в том числе CuteFTP, Go!Zilla, ReGet.

Известен также и перечень наиболее популярных «шпионов», услугами которых пользуются создатели программного обеспечения. Суперагентами сегодня считаются программы-шпионы Radiate, Cydoor и Web3000. Все они попадают на компьютер с довольно известными продуктами. Так, например, Radiate используют разработчики программ Gif Animator, Go!Zilla, GetRight и ReGet. Cydoor вы получаете в нагрузку к Audio CD MP3 Studio 2000, PC-to-Phone и ReGet. A Web3000 попадает на ваш компьютер вместе с NetCaptor, NetSonic и NetMonitor.

Антишпионские программы содержат в своих базах данных сведения о 200300 программах, относящихся к классу spyware.

Сегодня в связи с развитием сетевых технологий все большее распространение получает специфический вид программ-шпионов – так называемый бэкдор (транслитерация от англ. backdoor – «черный ход»).

Бэкдор – это программа, позволяющая удаленно управлять компьютером. Она может, например, изменить параметры рабочего стола, скорректировать права доступа пользователей компьютера, инсталлировать или, наоборот, удалить установленное программное обеспечение и т. п. Изначально подобная технология была разработана с целью облегчения жизни системных администраторов, но.

Каким образом бэкдор может попасть на компьютер пользователя? Так же, как и любая другая вредоносная программа.

При первом запуске бэкдор скрытно устанавливает себя в операционную систему и затем следит за действиями пользователя, не выдавая никаких сообщений. Более того, запущенный бэкдор может отсутствовать в перечне активных приложений. В результате владелец компьютера не знает о присутствии в системе программы удаленного администрирования, в то время как его компьютером может удаленно управлять злоумышленник.

В качестве примера относительно «свежего» бэкдора (появился в августе 2005 года) можно назвать Backdoor.Win32.Haxdoor.dw. После запуска он создает в системном каталоге Windows несколько файлов (avpx32.dll, avpx32.sys, avpx64.sys, p3.ini, qy.sys, qz.dll и qz.sys), а также изменяет системный реестр таким образом, чтобы обеспечить свой автоматически запуск при каждой последующей загрузке Windows. Будучи запущенным на выполнение, бэкдор открывает несколько портов зараженного компьютера и ожидает подключения машин-клиентов «хозяев» вредителя), которые затем могут отдавать ему команды на похищение паролей, системной информации, различных файлов и выполнение других несанкционированных действий. В частности, по команде «хозяина» бэкдор может просматривать список активных процессов, завершать некоторые из них и отсылать злоумышленнику найденную информацию.

Небольшое отступление, косвенно связанное со сказанным выше. Многие известные программы имеют в своем составе недекларированные возможности, часто называемые *пасхальными яйцами.* Чтобы активизировать такую скрытую функцию, следует знать специальный «ключик». Вот лишь один пример.

В «недрах» редактора электронных таблиц MS Excel 2000 спрятана трехмерная игра с условным названием «Автогонки» (кадр из нее приведен на рис. 1.3).

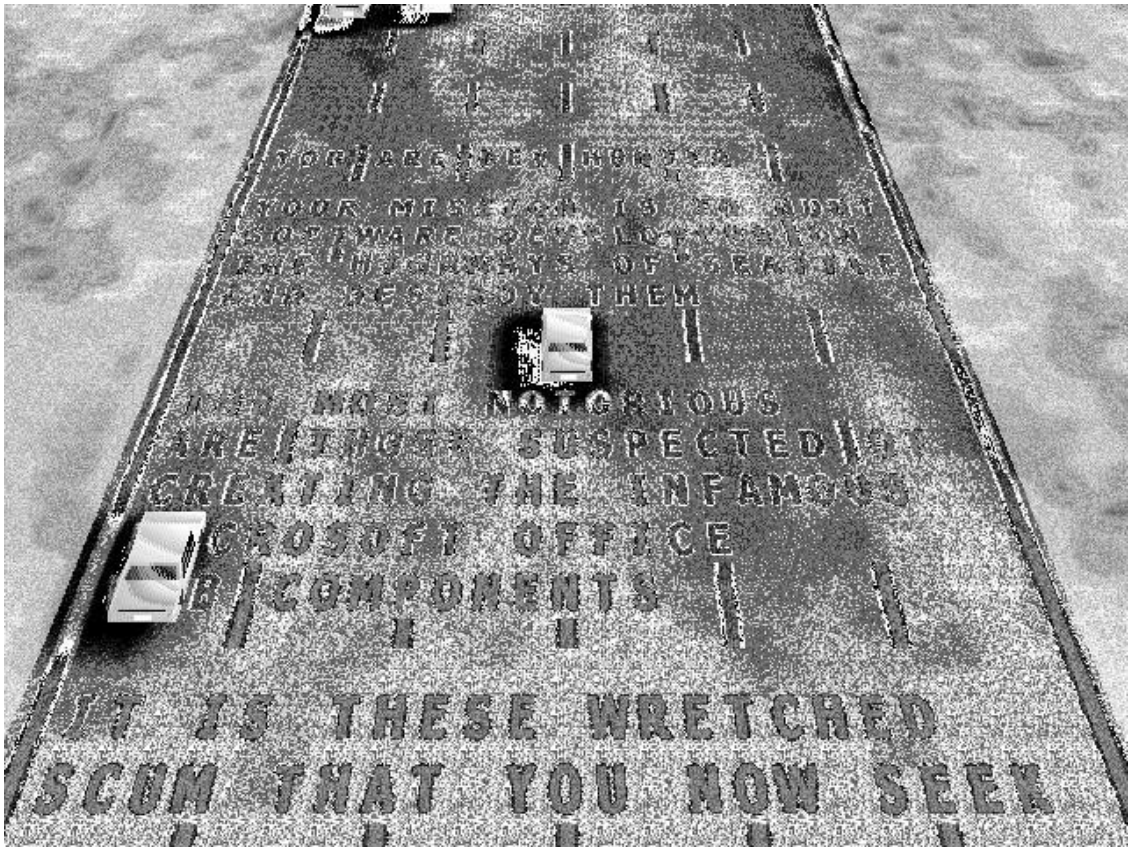


Рис. 1.3. «Шпионская» игра

Для запуска игры требуется выполнить следующие манипуляции.

1. Откройте MS Excel 2000, и в меню Файл выберите команду Создать ► Новая книга.

2. С помощью команды Файл ► Сохранить как Веб-страницу откройте диалоговую панель сохранения файла, поставьте в ней переключатель выделенное: Лист и флажок Добавить интерактивность; укажите маршрут сохраняемого файла.

3. Откройте созданный файл в браузере MS Internet Explorer (версия не ниже 5.0).

4. Во внедренном в HTML-страницу листе Excel найдите и выделите строку под номером 2000.

5. С помощью клавиши Tab сделайте активной ячейку этой строки в столбце WC (именно с помощью клавиши, не используя мышь).

6. Нажав и удерживая клавиши Ctrl+Alt+Shift, щелкните левой клавишей мыши на значке MS Office в левом верхнем углу внедренного окна Excel.

Приведенный пример наглядно демонстрирует непредсказуемость поведения всего того, что некоторые товарищи беспечно устанавливают на свои компьютеры.

Глава 2
Стратегия защиты и восстановления данных

У некоторых читателей может возникнуть вопрос: начинается уже вторая глава книги, а ни один рецепт по восстановлению данных еще не приведен. В чем дело?

Дело в том, что восстановление данных – это лишь одна из частей общей технологии защиты компьютерных данных. Как известно, любую болезнь проще предупредить, чем вылечить. Поэтому прежде, чем мы перейдем к «рецептам», рассмотрим основные профилактические средства, которые способны уберечь вас от потери данных.

Стратегия защиты данных должна быть направлена на противодействие наиболее вероятным случайным и умышленным угрозам. Реализация такой стратегии основана на трех «китах»:

обеспечении бесперебойного электропитания компьютера;

правильной настройке системных параметров;

применении средств резервного копирования и другого «защитного» программного обеспечения.

В данной главе рассматриваются средства обеспечения бесперебойного электропитания компьютера, а также виды «защитного» программного обеспечения (за исключением программ для резервного копирования). Технологии резервного копирования посвящена отдельная, четвертая глава книги. Вопросы настройки системных параметров рассмотрены в главе 3.

Обеспечение бесперебойного электропитания

Казалось бы, имея резервные копии всех данных, размещенные на резервных (опять же) носителях, можно избежать всех возможных неприятностей. Однако внезапное отключение электричества или броски напряжения могут привести не только к выходу из строя критически важных компонентов компьютера, но и к потере резервных копий (если проблемы с электричеством возникнут в момент создания этой самой резервной копии).

Необходимо отметить, что лишь около 20 % скачков напряжения бывают вызваны ударами молнии или проблемами у энергетиков. Большинство же энергетических импульсов исходит от копировальных аппаратов, принтеров, бытовых кондиционеров и другой офисной техники (равно как и от бытовых электроприборов).

Виды защитных устройств

Минимальный уровень защиты от энергетических неприятностей обеспечивают так называемые сетевые фильтры.

Сетевой фильтр – это устройство, которое позволяет защитить компьютер только от импульсных помех, то есть от кратковременных (длительностью в несколько тысячных долей секунды) выбросов напряжения. Такие выбросы могут вызываться короткими замыканиями, молниями, коммутированием и работой мощных потребителей электроэнергии и т. д. Мощные импульсные помехи очень опасны, так как они могут полностью сжечь блок питания и даже электронные схемы компьютера, а также вывести из строя внешние устройства компьютера. Многие современные модели сетевых фильтров обеспечивают также защиту подключенных устройств от высокочастотных помех и от короткого замыкания. Однако от падения напряжения ниже некоторого допустимого уровня фильтр защитить не сможет.

Более глубокую защиту способны обеспечить *стабилизаторы.* Предназначенные для компьютеров стабилизаторы сочетают в себе функции сетевого фильтра и «обычного» стабилизатора напряжения. Они не только отфильтровывают импульсные помехи, но и поддерживают на выходе стабильное напряжение при колебаниях входного напряжения на 30–40 % (как в большую, так и в меньшую сторону). Впрочем, в последнее время компьютерные стабилизаторы применяются редко, так как по стоимости соизмеримы с источниками бесперебойного питания, а по возможностям существенно им уступают. В крайнем случае вы можете подключить компьютер к сети через сетевой фильтр и бытовой стабилизатор (если таковой у вас имеется). Мощность стабилизатора должна быть не менее 200 Вт.

Источники бесперебойного питания (ИБП), или UPS (Uninterrupted Power Supplied), обеспечивают наиболее полную защиту компьютеров от проблем электропитания. Они содержат аккумулятор, который позволяет поддерживать в течение некоторого времени (от 5 до 30 минут) работу компьютеров и других подключенных к ним устройств даже при полном отключении внешней электросети. За это время можно, по крайней мере, корректно завершить работу активных программ и сохранить обрабатываемые данные. Кроме того, многие современные ИБП способны защитить от скачков напряжения телефонную (модемную) линию.

Источники бесперебойного питания на сегодняшний день представляют собой практически идеальное решение проблем для владельцев домашних компьютеров, поэтому рассмотрим их несколько подробнее.

Источники бесперебойного питания

К основным характеристикам современных ИБП относятся следующие:

способ формирования выходного напряжения;

диапазон значений входного напряжения, для которого ИБП способен выполнять свои функции;

время перехода на питание от аккумулятора;

выходная мощность.

Три первые из указанных характеристик напрямую зависят от класса ИБП. В настоящее время представленные на рынке ИБП могут быть отнесены к одному из трех классов.

Резервные (Stand-by, либо Off-line UPS, рис. 2.1, *слева)* – наиболее простые ИБП; называются резервными потому, что переключаются на питание от батареи лишь при выходе напряжения питания сети за границы определенного диапазона (обычно 187–264 В). При этом напряжение может колебаться в пределах допустимого коридора. Недостатком таких ИБП является относительно большое время переключения на резервный источник (порядка 5-20 мс). Еще одним недостатком следует считать форму выходного напряжения при питании от батареи: вместо синусоиды выходное напряжение представляет собой или трапецию, или прямоугольник, что отрицательно сказывается на долговечности компьютера.

Линейно-интерактивные ИБП (Line-interactive, или Ferroresonant UPS, называемые иногда также гибридными ИБП, рис. 2.1, *справа)* представляют собой дальнейшее развитие резервных ИБП в направлении улучшения фильтрации входного напряжения и улучшения формы выходного напряжения. В них используется встроенный автотрансформатор, регулирующий напряжение в заданном диапазоне (обычно в пределах 15–25 % от номинала в обе стороны). Если входное напряжение выходит за пределы этого диапазона, ИБП переключается в режим работы от батарей. К недостаткам линейно-интерактивных ИБП можно отнести все недостатки класса off-line, хотя и с некоторыми оговорками: например, время перехода на питание от батареи у линейно-интерактивных ИБП заметно ниже (1–5 мс). Кроме того, иногда, в силу наличия сложных фильтров и цепей обратной связи в линейно-интерактивных ИБП, возможно возникновение устойчивых искажений выходного сигнала, что является недопустимым в критичных областях применения компьютеров (например, в медицинском оборудовании или в качестве серверов баз данных).

ИБП *двойного преобразования* (или On-line UPS) – в них энергия питающей сети до того, как поступить на выход ИБП, дважды преобразуется: сначала напряжение сети выпрямляется, затем постоянное напряжение корректируется до необходимого уровня, после чего выполняется обратное преобразование. Такой принцип работы позволяет ИБП защитить подключенную нагрузку практически от всех существующих неполадок в электросети: высоковольтных выбросов, всплесков напряжения, электромагнитных и радиочастотных помех, кратковременного повышения или понижения напряжения, искажения его формы, полного отключения электропитания и т. п. Кроме того, при переключении на аккумуляторные батареи полностью отсутствуют переходные процессы у выходного напряжения, благодаря чему такое переключение можно считать мгновенным. Единственным серьезным недостатком является стоимость онлайновых ИБП, которая заметно выше, чем у линейно-интерактивных или резервных, поэтому они редко применяются в домашних условиях.

Рис. 2.1. Источники бесперебойного питания: резервный (слева) и линейно-интерактивный (справа)

Большинство современных моделей резервных и линейно-интерактивных ИБП поставляются вместе со специальным программным обеспечением. Как правило, такое ПО позволяет контролировать и настраивать рабочие параметры ИБП (входное и выходное напряжение, частоту, емкость аккумулятора, уровень нагрузки, рис. 2.2.), а также корректно завершать работу компьютера при длительных или чрезмерных перебоях питания. Кроме того, некоторые из управляющих программ способны при возникновении сбоев в электропитании посылать предупреждающие сообщения по электронной почте или локальной сети.

Мощность ИБП, как правило, не зависит от их класса. Например, мощность линейно-интерактивных ИБП одной и той же модели может составлять от 200 до 1000 ВА. Знать мощность используемого ИБП необходимо потому, что она должна соответствовать потребляемой мощности подключаемой нагрузки. Причем как в большую, так и в меньшую сторону. Так, для многих ИБП мощность нагрузки должна составлять не менее 30 % от мощности ИБП. То есть приобретать ИБП с большим запасом по мощности не только экономически невыгодно, но и вредно.

ВНИМАНИЕ _____

Мощность ИБП традиционно измеряется в вольт-амперах (ВА), а не в ваттах (Вт). Объясняется это тем, что ИБП является источником энергии, а не потребителем. Чтобыпра-вильно соотнести мощность ИБП и потенциальную нагрузку, следует учитывать соотношение 1 ВА = 0,7 Вт. Например, нагрузка для ИБП мощностью 500 ВА не должна превышать 350 Вт. Кроме того, необходимо помнить, что к ИБП запрещается подключать лазерные принтеры, а также устройства, имеющие блоки питания с трансформаторами на входе. Это может привести к выходу из строя электронной «начинки» ИБП.

Виды защитного программного обеспечения

Проблема защиты данных от всевозможных угроз занимает сегодня всех, кто так или иначе связан с компьютерами – от рядовых пользователей до производителей компьютеров и программного обеспечения. И потому сегодня практически на любую компьютерную «болячку» есть свой программный «пластырь» (насколько он эффективен – это уже другой вопрос). Причем та регулярность, с какой появляются средства «нападения» и средства «защиты», иногда вызывает подозрение, что и те и другие создаются усилиями одних и тех же творческих коллективов. Но это так, к слову.

Программное обеспечение, пригодное для выполнения защитных функций, можно достаточно условно разделить на несколько видов:

программы контроля целостности данных;

антивирусные программы;

программные средства контроля и разграничения доступа;

программные средства сетевой защиты;

средства криптографической защиты;

программы для работы с жесткими дисками и сменными носителями.

Последний пункт носит весьма общий характер. К этой категории отнесены, в частности, программы резервного копирования и восстановления данных, а также программы для создания и изменения параметров файловой системы. Такое обобщение вызвано тем, что именно программам этой группы посвящены последующие главы книги.

Для других защитных программ далее приведена краткая характеристика с некоторыми рекомендациями по их практическому применению.

Программы контроля целостности данных

Из всего перечисленного выше «джентльменского набора» это наиболее простые программы. Даже и не программы, а утилиты, поскольку реализуют они, как правило, одну-единственную функцию: определяют факт изменения содержимого файла или папки.

Механизм работы таких программ основан на вычислении так называемой *контрольной свертки* – CRC (Cyclic Redundancy Check, дословно – «циклический избыточный контрольный код»).

ПРИМЕЧАНИЕ _____

Иногда аббревиатуру CRC интерпретируют как «контрольная сумма», что неверно, поскольку вычисление контрольной суммы для некоторого блока данных – это альтернативный метод проверки, более простой и менее надежный. Вычисление же CRC основано на применении специального «магического» полинома, коэффициентыкоторого определяются в соответствии с используемым алгоритмом CRC.

Обычно длина значения CRC составляет 16 или 32 двоичных разряда. 32-разрядную контрольную свертку для определенности обозначают CRC32, а само значение представляют в шестнадцатеричном коде.

Использование CRC32 обеспечивает очень высокую достоверность контроля. Достаточно изменить единственный бит в контролируемом файле, и значение контрольной свертки станет совершенно другим. Например, взгляните на значения CRC32 для двух текстовых файлов, различающихся одним битом (рис. 2.3).

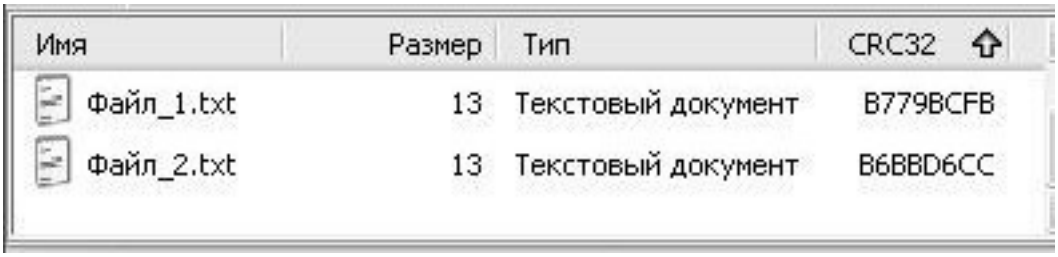
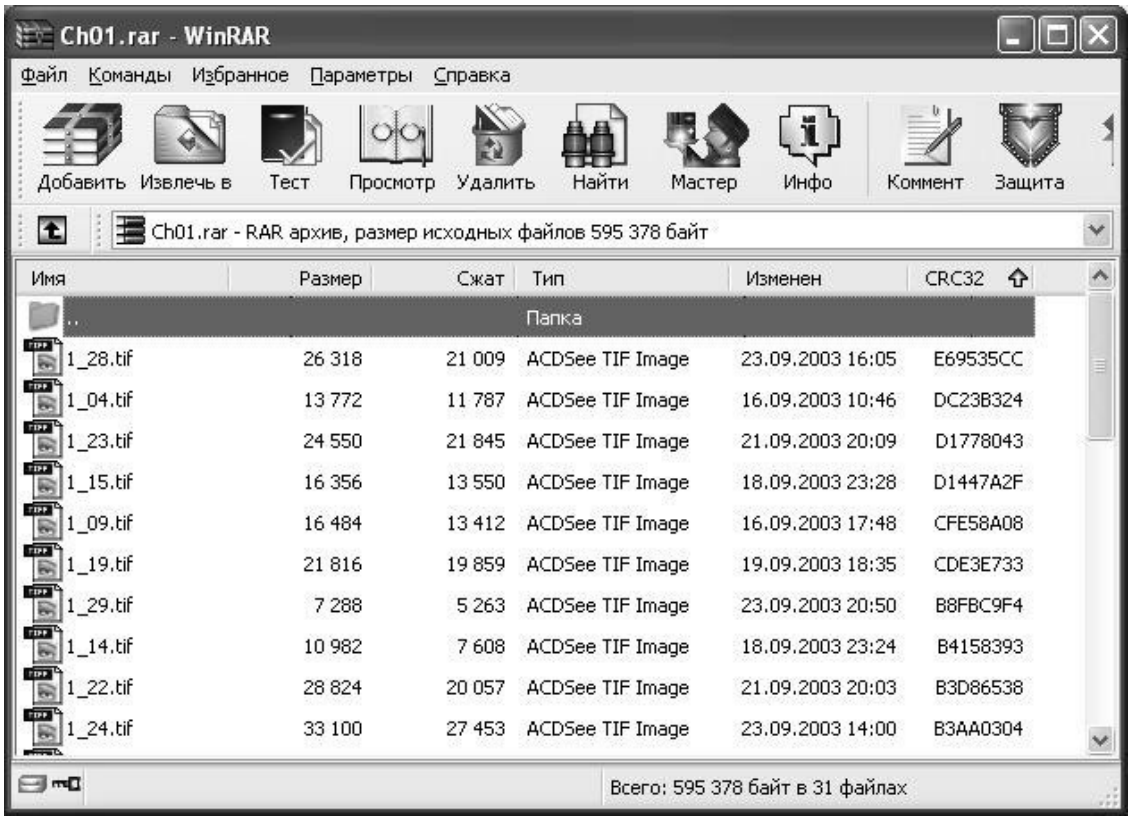


Рис. 2.3. Значения CRC32 для двух файлов

Известно достаточно много программ, обеспечивающих контроль целостности данных на основе вычисления CRC. Большинство из них бесплатны или условно-бесплатны. В разных программах могут использоваться различные алгоритмы вычисления CRC, однако принцип работы один: сначала программа вычисляет контрольную свертку для каждого из указанных файлов (или папок), а затем при повторном запуске выполняет повторный расчет CRC и сравнивает полученное значение с тем, которое хранится в базе данных программы.

Необходимо отметить, что утилиты контроля целостности данных на основе CRC входят в состав более сложных и мощных защитных программ. В частности, анализ CRC контролируемых файлов выполняют антивирусные пакеты (с целью выявления факта несанкционированного изменения этих файлов). В программах-архиваторах CRC используется для контроля целостности архива (рис. 2.4).



Антивирусные программы

На сегодняшний день перечень доступных антивирусных программ весьма обширен. Они различаются как по цене (от весьма дорогих до абсолютно бесплатных), так и по своим функциональным возможностям. Наиболее мощные (и, как правило, наиболее дорогие) антивирусные программы представляют собой на самом деле пакеты специализированных утилит, способ-

ных при совместном их использовании поставить заслон практически любому виду зловредных программ.

Вот типовой (но, возможно, неполный) перечень тех функций, которые способны выполнять такие антивирусные пакеты:

сканирование памяти и содержимого дисков по расписанию;

сканирование памяти компьютера, а также открываемых и записываемых файлов в реальном режиме времени с помощью резидентного модуля;

выборочное сканирование файлов с измененными атрибутами;

распознавание поведения, характерного для компьютерных вирусов;

блокировка и/или удаление выявленных вирусов;

восстановление зараженных информационных объектов;

принудительная проверка подключенных к корпоративной сети компьютеров;

удаленное обновление антивирусного программного обеспечения и баз данных с информацией о вирусах, в том числе автоматическое обновление вирусных баз данных через Интернет;

фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;

выявление потенциально опасных Java-апплетов и модулей ActiveX;

ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты.

К наиболее мощным и популярным на сегодняшний день (в России) антивирусным пакетам относятся:

Doctor Web (Dr Web) – программа российской компании «ДиалогНаука» (www.dialognauka.ru);

Антивирус Касперского (AVP) – разработка российской фирмы «Лаборатория Касперского» (www.kaspersky.ru);

Norton Antivirus корпорации Symantec; сайт компании (www.symantec.com) имеет русскоязычный раздел;

McAfee VirusScan компании Network Associates (www.mcafee.ru);

Panda Antivirus компании Panda SoftWare (www.pandasoftware.com).

Популярность перечисленных выше пакетов обусловлена прежде всего тем, что в них реализован комплексный подход к борьбе с вредоносными программами. То есть, установив такой пакет на своем компьютере, вы избавляетесь от необходимости использовать дополнительные антивирусные средства.

> ПРИМЕЧАНИЕ
>
> Последние версии антивирусных пакетов содержат также средства борьбы с вредоносными программами, проникающими из сети. Тем не менее специализированные инструменты отражения сетевых угроз рассматриваются отдельно.

Так какие же, собственно, существуют технологии выявления и нейтрализации компьютерных вирусов?

Специалисты в области антивирусной защиты (в частности, Е. Касперский) выделяют пять типов антивирусов, реализующих соответствующие технологии:

сканеры;

мониторы;

ревизоры изменений;

иммунизаторы;

поведенческие блокираторы.

Сканеры

Принцип работы *антивирусного сканера* состоит в том, что он просматривает файлы, оперативную память и загрузочные сектора дисков на предмет наличия *вирусных масок,* то есть уникального программного кода вируса. Вирусные маски (описания) известных вирусов содержатся в антивирусной базе данных сканера, и если он встречает программный код, совпадающий с одним из этих описаний, то выдает сообщение об обнаружении соответствующего вируса.

ПРИМЕЧАНИЕ

В качестве маски вируса обычно используется так называемая сигнатура, то есть характерная для данного вируса последовательность байтов.

Недостаток любого сканера заключается в том, что он не способен обнаруживать новые (неизвестные) вирусы, о которых отсутствует информация в базе данных сканера. Кроме того, сканер практически бессилен против *полиморфных* вирусов, каждая новая копия которых отличается от предыдущей.

Мониторы

Мониторы являются разновидностью сканеров. Монитор постоянно находится в памяти компьютера и осуществляет автоматическую проверку всех используемых файлов в масштабе реального времени. Современные мониторы проверяют программы в момент их открытия и закрытия. Благодаря этому исключается возможность запуска ранее инфицированных файлов и заражения новых файлов резидентным вирусом. Для включения антивирусной защиты достаточно загрузить монитор при запуске операционной системы или приложения. Как правило, это делает сам антивирусный пакет в процессе его установки. В случае обнаружения вредоносной программы монитор, в зависимости от настроек, «вылечит» файл, заблокирует его выполнение или изолирует, переместив в специальную «карантинную» папку для дальнейшего исследования.

В настоящее время используются мониторы трех типов:

файловые мониторы;

мониторы для почтовых программ;

мониторы для специальных приложений.

Файловые мониторы работают как часть операционной системы, в масштабе реального времени проверяя все используемые объекты, вне зависимости от их происхождения и принадлежности какому-либо приложению.

Мониторы для почтовых программ интегрируются в программы обработки электронной почты (как серверные, так и клиентские) и при поступлении нового письма автоматически проверяют его.

Мониторы для специальных приложений также обеспечивают фоновую проверку объектов, но только в рамках приложения, для которого они предназначены. Типичный пример – мониторы для MS Office. Подобно своим «почтовым» «коллегам», они интегрируются в программу и находятся в памяти компьютера во время ее работы.

Ревизоры

Принцип работы *ревизоров изменений* основан на вычислении для файлов, системных секторов и системного реестра контрольных сверток (CRC). Они сохраняются в базе данных ревизора, и при следующем запуске ревизор сверяет «отпечатки» с их оригиналами и сообщает пользователю о выявленных отклонениях, обращая особое внимание на вирусоподобные изменения. При использовании ревизоров «лечение» зараженных объектов основывается не

на опознании конкретного вируса, а на знании того, как должен выглядеть «чистый» файл или сектор: любые отклонения от эталона регистрируются ревизором, который способен вернуть объект к исходному состоянию.

Однако у ревизоров изменений имеются свои недостатки. Во-первых, они не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время, уже после того, как вирус заразит хотя бы один объект. Во-вторых, они не могут определить вирус в новых файлах, поскольку для таких файлов в базе данных ревизора отсутствует эталонное значение CRC.

Иммунизаторы

Иммунизаторы, которые иногда называют также *вакцинами,* действуют подобно медицинским вакцинам: они помещают в тело информационного объекта специальные метки, препятствующие их настоящему заражению вирусом.

Иммунизаторы бывают двух типов: *информирующие* и *блокирующие.*

Первые обычно записываются в конец файлов (по принципу файлового вируса), и каждый раз при запуске файла проверяют его на изменение. Такие иммуниза-торы имеют один существенный недостаток: они не способны обнаружить заражение вирусами-невидимками.

Иммунизаторы второго типа защищают систему от заражения определенным вирусом. Блокирующий иммунизатор помечает файлы таким же образом, как и нейтрализуемый вирус, благодаря чему тот считает их уже зараженными. Например, чтобы предотвратить заражение COM-файла вирусом Jerusalem, достаточно дописать в конец файла строку MSDos. Для защиты от резидентного вируса в память компьютера заносится программа, имитирующая копию вируса. При запуске вирус обнаруживает ее и считает, что система уже заражена.

Конец ознакомительного фрагмента.