"ГЛЮКИ"

СБОИ И ОШИБКИ КОМПЬЮТЕРА

Решаем проблемы сами

Жуховцев Д.М.,
Прокди Р.Г.,
Финкова М.А.

2-е издание

Эта книга - спасательный круг для вашего компьютера

НиТ издательство

ГЛЮКИ, СБОИ И ОШИБКИ КОМПЬЮТЕРА

Жуховцев М. Д., Прокди Р. Г., Финкова М. А. и др.

«ГЛЮКИ», СБОИ И ОШИБКИ КОМПЬЮТЕРА. РЕШАЕМ ПРОБЛЕМЫ САМИ. 2-Е ИЗД. СПб.: Наука и Техника, 2013. — 240 с., ил.

Серия «Просто о сложном»

Данная книга послужит вам спасательным кругом во многих критических ситуациях, которые могут возникнуть с компьютером: ваш компьютер не загружается, компьютер «тормозит», в системе происходят постоянные «глюки» и сбои, не воспроизводится видео, пропал звук, при включении компьютера раздаются «пищащие» звуки, а загрузка Windows не происходит, и многое другое. Отдельная глава посвящена распространенной в последнее время проблеме блокировки компьютера. Когда все действия на компьютере заблокированы, а на экране отображается надпись с просьбой отправить платное СМС на определенный номер, и тогда вам придет код разблокировки. Так вот, в книге рассказывается, как самим разблокировать компьютер без уплаты денег (кстати, иногда после отправки СМС ничего не происходит, и компьютер так и остается заблокированным). Аналогичная проблема рассматривается для случаев блокировки вашей странички ВКонтакте и Одноклассниках.

Есть глава, посвященная проблеме нечитающихся дисков CD и DVD. Есть глава, посвященная восстановлению работоспособности Windows. Есть глава, посвященная решению проблем автоматически запускаемых программ и нежелательных процессов в системе. Есть глава... Да много еще чего есть! И все в виде понятных пошаговых инструкций без лишних подробностей. Книга будет несомненно полезна всем пользователям компьютеров!

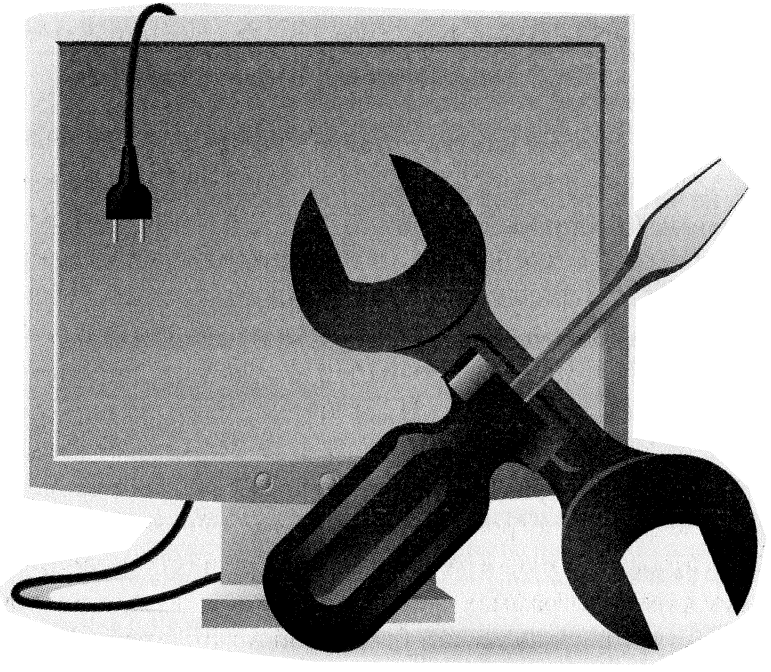
Контактные телефоны издательства:
(812) 412 70 25, (812) 412 70 26, (044) 516 38 66

Официальный сайт: www.nit.com.ru

Содержание

ГЛАВА 1.

ОТКУДА БЕРУТСЯ СБОИ И КАК ИХ ИЗБЕГАТЬ



1.1. Две дороги, два пути

Прежде чем перейти к конкретным действиям, настройкам и рекомендациям, необходимо определиться, чего же мы собственно хотим. Как говорится, обозначить цель. А целью нашей является стабильная работа компьютера и установленного на нем программного обеспечения, а также сохранность ваших данных (файлов) и уверенное выполнение всех тех задач, которые решаются на компьютере. Причем желательно все это иметь не только сегодня, завтра и послезавтра, но и в течение достаточно длительного промежутка времени (год-два-три, а то и больше).

Конечно, если вы пользуетесь компьютером раз в год по обещанию, то надо сильно постараться, чтобы угрохать свой компьютер за несколько сеансов работы (хотя дурное дело нехитрое). В то же время, если компьютер используется достаточно часто, практически ежедневно, то длительное поддержание его в работоспособном состоянии – задача не из самых простых. Особенно если вы «отрываетесь на всю катушку»: устанавливаете различные программы, активно пользуетесь Интернетом, часто обмениваетесь файлами, работаете в локальной сети и т.д. При таком раскладе, если не соблюдать определенных профилактических мер, не произвести некоторые настройки и не пользоваться дополнительным специализированным программным обеспечением (антивирусом, брандмауэром, программами-Uninstaller'ами и т.п.), достаточно быстро наступит конец вашей беспечной компьютерной жизни. Компьютер станет тормозить, что-то там сам с собой делать, часто «задумываться», выполнять незапланированные действия, выдавать ошибки, перезагружаться, а то и портить файлы. Кроме того,

не следует исключать и аппаратные проблемы, то есть проблемы с внутренними устройствами компьютера.

На фоне этого всего в компьютерной практике можно выделить два способа поведения пользователя при работе на компьютере. Одни пользователи ни о чем не заботятся, делают, что себе вздумается, и в результате получают вышеописанный букет «веселых» компьютерных болезней. По мере появления все новых и новых симптомов, они какое-то время терпят их: ну подумаешь, система стала 5 минут загружаться, ну подумаешь, компьютер «виснет» через каждый час – ведь этот же час можно что-то поделать, а за пять минут загрузки можно выпить стакан чая. Но наступает момент, когда чаша терпения переполняется и такие пользователи просто-напросто сносят систему со всем установленным в ней добром и устанавливают ее заново. А после установки все повторяется снова, до следующей переустановки...

В какой-то степени это один из вполне приемлемых путей. Основным и единственным плюсом такой «жизни» является отсутствие необходимости что-либо делать по настройке компьютера, как-то заботиться о его работоспособности. Минусов же очень много:

- из-за постоянно появляющихся «глюков» полноценной работа на компьютере при таком подходе перестает быть уже достаточно быстро,

- из-за сбоев начинают пропадать если не файлы с диска, то результаты вашей последней работы (например, программа «зависла» после двух часов работы, и все, что вы за это время в ней сделали, пропало)

- процесс переустановки достаточно длителен (особенно если сюда добавить переустановку всех программ), а после

переустановки многие настройки пропадают, а вы не помните, как у вас это было настроено...

- многие проблемы возвращаются и после переустановки (например, завирусованные файлы при переустановке никуда не деваются и при попытке ими воспользоваться, вы получите снова вирусные проблемы...).

Другой путь заключается в том, чтобы... следовать совету врачей. А что нам говорят врачи? Они говорят: «Следите за собой. Профилактика эффективнее, лучше и дешевле лечения». То же самое и с компьютером. Соблюдайте меры профилактики, следите за настройками, периодически «сдавайте анализы» (проверяйте, что у вас творится в системе), – и все будет хорошо! Подобный путь во всем лучше, полезнее и эффективнее. Единственный его минус заключается в человеческой лени. Как лень бывает почистить зубы или побриться, так лень бывает установить антивирусную программу, раз в неделю проверять систему, следить за ее настройками. И если с чисткой зубов мы все как-то примирились (особенно после пары посещений стоматолога), то с компьютером эту лень еще надо преодолеть. А человек, как признано им самим, – животное ленивое.

Итак, будем считать, что вы решили встать на путь истинный. А с данной книгой вы поймете, что это совсем несложно. Многие настройки следует произвести лишь один раз, а эффект от них будет благоприятно сказываться на работоспособности компьютера все время. Помимо профилактических мер, в рамках данной книги мы с вами узнаем, как правильно и эффективно бороться с возникающими компьютерными проблемами и сбоями. К сожалению, полностью их исключить невозможно, а неправильное решение той или иной проблемы может повлечь за собой целый ворох других. Вы научитесь следить за работой компьютера (систе-

мы, программ) и уже на раннем этапе пресекать зачатки будущих проблем и сбоев.

1.2. Что нужно, чтобы компьютер долгое время работал стабильно, без проблем и без сбоев

Чтобы обеспечить максимально долгую и стабильную работу компьютера, лучше всего на нем ничего не делать. Это как с автомобилем: чтобы он дольше сохранился в целостности и сохранности, лучше на нем не ездить. Однако, зачем он нам тогда вообще нужен? Мы с вами собираемся на компьютере делать кучу всего и вообще эксплуатировать его «по полной». Поэтому нам подобное «мудрое» правило не подходит.

Максимально обеспечить стабильную работу компьютера (и системы) при полноценном его использовании позволяет следующий набор средств и настроек:

1. Использование антивирусной программы – для защиты от вирусов.

2. Использование программы-брандмауэра (он же файерволл) – для защиты от сетевых атак и нежелательной сетевой активности. Имеет смысл, если вы подключаетесь к Интернету.

3. Грамотные установка и удаление программ. Причем удаление желательно осуществлять с помощью какой-либо специальной программы (Uninstaller'а – читается как *анинсталлер'а*), а не стандартными средствами, так как в последнем случае в системе остается много следов, которые могут служить источником последующих проблем.

4. Контроль за происходящими в системе процессами.

5. Использование только проверенных программ из проверенных источников. Если у вас изначально поврежденная пиратская версия операционной системы, с внедренными в нее вредительскими закладками, то проблем не избежать, а чтобы с ними бороться, понадобятся усилия.

6. Грамотное решение возникающих проблем – чтобы они не послужили источником других.

7. Установка всех необходимых драйверов.

8. Грамотная настройка операционной системы и установленных программ. Например, рекомендуется отключать неиспользуемые службы Windows, чтобы они, во-первых, не отъедали системных ресурсов, а во-вторых, не были потенциальным источником проблем. Как говорил Аль Капоне: «Нет человека, нет проблемы». Так и тут: если служба отключена, то она не может служить источником бед. В то же время Windows по умолчанию запускает достаточно большое количество ненужных служб (типа на всякий случай).

Желательно также следить за появлением обновлений установленных у вас системы и программ и по возможности устанавливать их.

1.3. Какие средства предусмотрены для борьбы с уже возникшими компьютерными проблемами и сбоями

Для борьбы с компьютерными проблемами и сбоями вам прежде всего понадобится ваша голова. Бездумное и слепое использова-

ние того или иного средства может либо не помочь, либо привести к еще более худшему результату. Если же говорить более предметно, то можно выделить определенный набор компьютерных технологий и путей, позволяющих решать наибольшее количество проблем и сбоев в случае их возникновения. При этом в рамках решения каждой проблемы необходимо различать два этапа:

- идентификация проблемы (определение того, что и как сломано), выявление ее причины;
- собственно решение проблемы.

Далее приведен перечень стандартных средств и инструментов для обоих этапов вместе:

1. **BIOS**. В случае проблем с загрузкой компьютера либо на экране выдается сообщение с названием ошибки, либо системный динамик (пищалка внутри компьютера) подает соответствующую комбинацию коротких и длинных гудков, по которым можно идентифицировать ошибку и принять меры.

2. При загрузке операционной системы Windows может появляться так называемый **синий экран смерти**, на котором приводится код ошибки и даются краткие пояснения. Более подробную информацию и рекомендации по каждой конкретной ситуации можно получить в Интернете по коду ошибки. Многие из них рассмотрены в гл. 9 книги.

3. **Инструмент восстановления Windows**, встроенный в саму Windows (см. гл. 8) и позволяющий «откатить» систему в пре-дыдущее стабильное состояние. Бывает полезно, если сбои начали появляться после установки какой-либо программы или проведения каких-либо настроек.

4. Хорошо развитое **Интернет-сообщество**. В Интернете существует большое количество сайтов (форумов), на которых можно задать вопрос, и на него вам ответят. Кроме того, вполне вероятно с подобной проблемой сталкивался еще кто-то, и вы сразу сможете найти уже готовое нужное решение.

5. **Диспетчер задач** – позволяет следить за выполняемыми в системе процессами и в случае необходимости пресекать их активность (см. п. 7.2). Если Windows (и компьютер вообще) стала «тормозить» или вытворять что-то непонятное, то вполне вероятно, что виной тому является какой-либо из процессов (возможно, зловредный). Соответственно если его отключить, то и проблема исчезнет.

6. **Реестр Windows** – база данных, в которой хранится информация обо всех настройках и параметрах работы Windows, а также конфигурация всех установленных в системе приложений. Через редактирование реестра можно решить достаточно много проблем, однако это требует специальной подготовки/знаний, и его рассмотрение выходит за рамки данной книги.

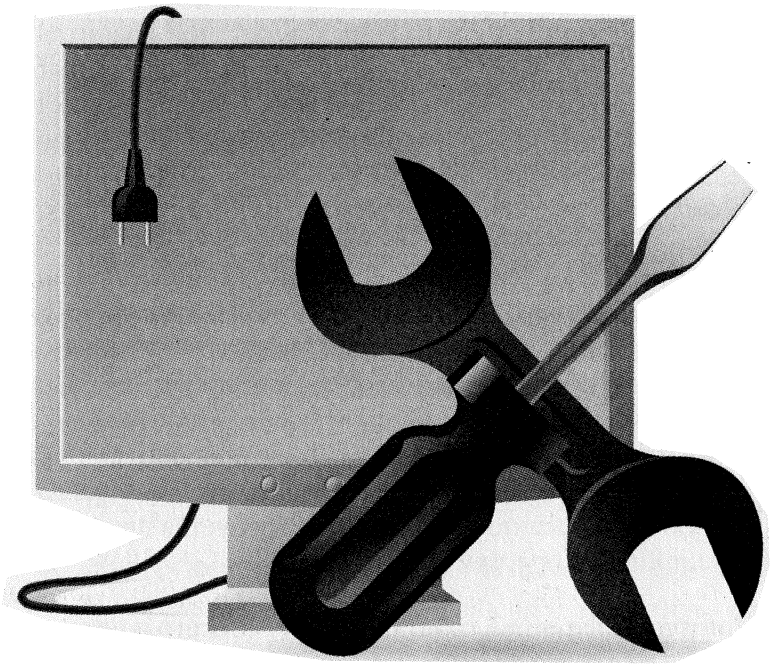
7. **Установка заплат и обновлений**. Довольно часто избавиться от той или иной проблемы позволяет установка заплатки или обновления к проблемной программе. Подобные заплаты/обновления выпускаются почти для всех программ их производителями. Доступны они, как правило, на интернет-сайте фирмы производителя. Правда, зачастую для успешного обновления требуется проверка лицензионности программы.

8. **Комплексные меры**, сочетающие в себе всего понемножку.

9. **Специализированные программы**, призванные решать те или иные проблемы (восстановление данных, тестирование устройств компьютера и т.п.).

ГЛАВА 2.

САМЫЕ РАСПРОСТРАНЕННЫЕ МЕЛКИЕ «ГЛЮКИ» И ПРОБЛЕМЫ С КОМПЬЮТЕРОМ



Компьютер не включается

Ситуация: вы нажимаете кнопку включения (кнопку «Power») на компьютере, а компьютер не включается. В данной ситуации очень важны детали. Давайте разбираться. Если вообще ничего не происходит, то здесь дело в электропитании компьютера. Скорее всего, проблемы с блоком питания, а может быть, вы просто забыли включить компьютер в розетку. Если же с розеткой все в порядке, то проверьте, не выскочил ли кабель питания из гнезда сзади системного блока компьютера. Кроме того, сзади компьютера, недалеко от того места, куда вставлен кабель питания, должен располагаться переключатель, который включает и отключает блок питания. Если этот переключатель находится в выключенном состоянии, то сколько бы вы ни нажимали кнопку «Power», ничего не произойдет. Попробуйте переключить переключатель в другое положение и снова загрузить компьютер. Если же все вышеперечисленные действия не привели ни к какому результату, то вам, скорее всего, необходимо заменять блок питания в системном блоке. Он у вас «сгорел». Отметим, что к этому печальному исходу может привести большое содержание пыли.

Другое дело, если компьютер не включается, но при попытке включения издает несколько звуков-гудков. О том, что это значит, сказано в гл. 11 данной книги.

На экране нет изображения, но системный блок «шумит»

В данной ситуации проблема либо с монитором, либо с видеокартой внутри системного блока. На всякий случай также проверьте, надежно ли вставлен кабель, соединяющий системный блок с монитором. Случаи, что причина в мониторе, довольно редки. Монитор никогда не «умирает» быстро. Обычно он сначала начинает показывать плохо цвета, начинает дрожать изображение и т.д. Вот что случается часто, так это то, что монитор выключают, а по-

том забывают об этом, ожидая, что он автоматически включится при включении компьютера. Найдите кнопку включения/выключения монитора и нажмите ее. Попробуйте включить компьютер снова. Возможно, проблема разрешится. Наконец, проверить, рабочий у вас монитор или нет, можно, подключив его к другому системному блоку.

Вы проверили кабель, вы проверили монитор, все работает. Тогда вам нужно заменять видеокарту. Это устройство отвечает за передачу видеоинформации из системного блока на монитор. Вам придется купить новую и заменить.

Компьютер стал «тормозить», очень медленно работать, стали появляться глюки

Проблема это очень обширна, и причин ее может быть множество. Основные же из них, на которые приходится 80% всех случаев, таковы:

- в системе завелся вирус;
- в системе стало очень много программ запускаться автоматически (при загрузке компьютера) – решение проблемы см. п. 6.3.;
- в системе стало много запускаться ненужных процессов – решение проблемы в гл. 7.;
- вы давно не перезагружали компьютер, оставляя его постоянно включенным, – сделайте это,
- система стала очень замусорена множеством настроек, установок и проч. – о решении проблемы читайте в гл. 6.;
- на логическом диске, на который установлена система Windows (где находится папка Windows), осталось мало свободного места – удалите ненужные файлы;

- система заражена вирусом – необходимо запустить проверку ВСЕГО компьютера (а не отдельных файлов). Для этого необходимо вызвать основное окно Антивируса (выполнив двойной щелчок мышью по его значку) и оттуда запустить проверку. Подобная проверка может занять несколько часов, поэтому лучше ставить ее на ночь;

- система стала плохо себя вести после установки какой-либо программы. Необходимо восстановить систему в том состоянии, в котором она пребывала до установки программы. Об этом сказано в гл.

Одним из самых действенных способов реанимации Windows (а то, что компьютер стал тормозить, это следствие сбоев в системе) является ее восстановление или откат к одному из предыдущих работоспособных состояний. Об этом сказано в гл. 8. Если же ничего не помогает, то вам придется переустановить систему. Это довольно трудоемкий процесс, описание которого занимает целую книгу. Поэтому лучше довериться специалисту либо купить соответствующую книгу.

Компьютер после включения автоматически выключается через несколько минут

Внутри компьютера что-то перегревается. Чаще всего это связано с тем, что забивается пылью вентилятор (кулер), охлаждающий процессор, видеокарту или материнскую плату. Необходимо как можно быстрее открыть системный блок и почистить его от пыли внутри, убедиться, что все вентиляторы крутятся нормально. Лучше всего чистку делать пылесосом, только не протирайте ничего мокрой тряпкой. Сделать это нужно как можно быстрее, иначе устройство может перегореть. Если же чистка не помогла, значит уже поздно. Устройство необходимо менять.

Не показывается фильм

Данная проблема встречается все реже и реже. Однако, если это с вами случилось, знайте: у вас в системе нет кодека для воспроизведения этого видео. Выход простой: установить кодек. Чтобы не искать, какого именно кодека вам не хватает, установите сразу все кодеки. Гарантированный результат дает установка пакета кодеков K-Light Codec Pack (например, можно взять здесь: http://www.codecguide.com/download_kl.htm).

Не работает клавиатура

Вы не поверите, но чаще всего проблемы с клавиатурой связаны с тем, что либо клавиатура отключена от компьютера, либо на клавиатуру что-то вылили. Действия и в том и в том случае очевидны.

После вставки CD или DVD компьютер завис

Причина в том, что компьютеру не удалось сходу прочитать данные с вставленного диска. Он пытается менять скорость чтения и вообще как-то решить проблему. При этом компьютер по сути находится в «зависшем» состоянии. Вам нужно либо подождать, пока диск не прочитается, либо извлечь диск.

Не устанавливается программа

Довольно часто установка какой-либо программы конфликтует с одной из уже существующих программ. При этом недостаточно будет просто удалить эту программу. Необходимо будет также «зачистить» и следы пребывания этой программы у вас на компьютере. О том, как это сделать, читайте в гл. 6. Кроме того, довольно часто программа нуждается в установке специальных файлов (так называемых библиотек). Обычно все это указыва-

ется в системных требованиях в описании игры или на обратной стороне ее коробки.

Пропал звук

Основными причинами являются следующие: колонки подключены не к тому гнезду на задней стенке компьютера, переключатель на звуковой колонке находится в выключенном положении, уровень громкости стоит на нуле, колонки неисправны (реже всего), звуковая карта неисправна. Бывает, что причиной «пропажи» звука является USB-микрофон, подключенный к USB-порту компьютера. Просто отключите его и перезагрузите компьютер.

Регулярно происходит сбой даты

На материнской плате внутри системного блока имеется маленькая батарейка, благодаря которой в компьютере сохраняются основные базовые настройки. Именно их считывает компьютер при включении и в соответствии с ними производит загрузку. Если же батарейка начинает садиться, то настройки начинают периодически сбрасываться к «заводским» значениям. Дата также относится к этим настройкам. Вам нужно самим, или попросить кого-нибудь, найти эту батарейку, купить такую же и заменить ее.

Компьютер стал сильно «шуметь»

Это связано с тем, что забились пылью вентиляторы внутри компьютера. Нужно как можно скорее открыть системный блок (не забыв его перед этим отключить от электросети) и почистить от пыли. В противном случае шум вскоре закончится тем, что какое-либо устройство перегорит.

Перестали читаться диски CD и DVD

Причина может заключаться либо в устройстве чтения CD/DVD, либо в самом диске. Попробуйте свой диск прочитать на другом компьютере. Если это вам удалось, то надо менять CD/DVD-привод. Если же и на другом компьютере диск не прочитался, то проблема в диске. О способах, позволяющих считать данные с «плохих» CD и DVD, сказано в гл. 10

Не запускается игра

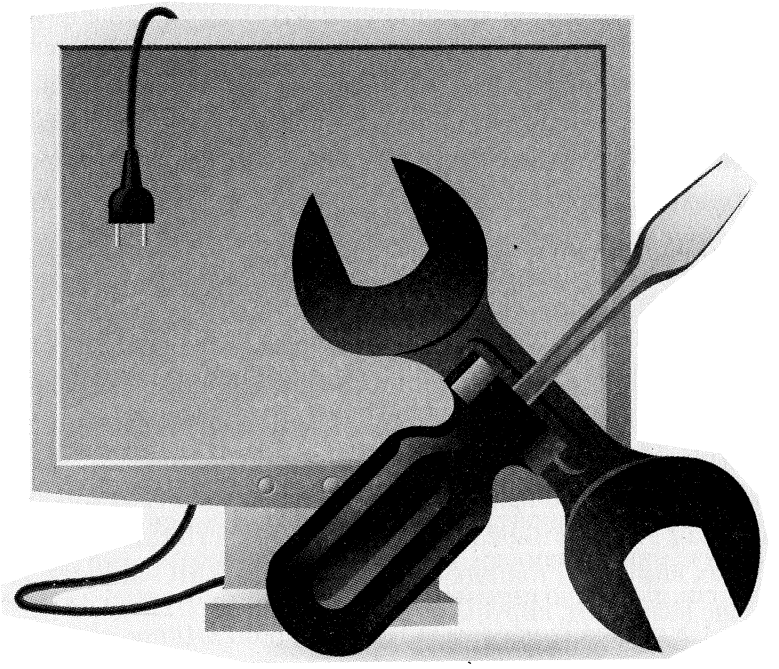
Причина заключается либо в том, что параметры вашего компьютера не удовлетворяют минимальным требованиям, предъявляемым программой, либо в том, что не хватает дополнительных программных библиотек. Обычно для игр указывается версия Direct X, и ее вам необходимо установить.

Программа «зависла»

Прежде всего, подождите и понаблюдайте, что происходит. Возможно, что программа вовсе не зависла, а что-то делает (просчитывает), но делает это очень медленно. Можно минут пять подождать. Если же ждать неохота, либо вы точно поняли, что это бесполезно, то щелкните правой кнопкой мыши по кнопке программы на панели задач и в появившемся контекстном меню выберите команду Закрыть. Или же можно нажать сочетание клавиш «Ctrl» + «Alt» + «Del». В появившемся окне на вкладке Приложения выбрать зависшую программу и нажать кнопку Завершить задачу. Если же вообще все «зависло» и нет реакции на движения мыши, то нужно перезагрузить компьютер, нажав на кнопку «Reset» на передней панели системного блока. Если такое происходит часто и с разными программами, то дело, скорее всего, в системе, и вам надо сначала ее почистить (гл. 6), а если не поможет – провести ее восстановление (гл. 8).

ГЛАВА 3.

ВАШ КОМПЬЮТЕР ЗАБЛОКИРОВАН, ОТ ВАС ТРЕБУЮТ ОТПРАВИТЬ SMS С ОПЛАТОЙ



Современные компьютерные вирусы прошли стремительный путь развития от безобидного приложения, выводящего на экраны компьютеров шутливое сообщение, распространяющееся по сети: «I'm the creeper, catch me if you can!»[1], до криминального бизнеса, жертвой которого может стать любой пользователь ПК.

Первые компьютерные вирусы писались, что называется, на коленке, любознательными школьниками, скучающими программистами. Цель экспериментов сводилась к тому, чтобы попробовать свои силы и блеснуть мастерством. Ни о каком хищении или преднамеренной порче данных и не велось речи. За несколько десятилетий ситуация в корне изменилось. На смену вчерашним школьникам пришли профессионалы, для которых компьютерный вирус стал универсальным ключом к любой информации на компьютере, независимо от его местоположения, а также источником финансовой прибыли.

Развитие Интернета и появление многочисленных социальных сетей только подлили масла в огонь. Из одиноко бродивших компьютерных вирусов образовался настоящий круговорот, в котором уже сложно классифицировать принадлежность компьютерного вируса к той или иной группе. Но все же есть категория компьютерных вирусов, стоящих особняком. Это СМС-вирусы, или, как их еще называют, вирусы вымогатели СМС.

Классический СМС-вирус блокирует работу операционной системы и требует ввести код активации, получить который можно

1 Я Крипер, поймай меня, если сможешь!

после отправки СМС на указанный номер. Как догадался читатель, СМС вовсе не бесплатное, а обещанный код активации может и не подойти. Не спешите отправлять сообщение по спасительному номеру! В нашей книге вы найдете рецепты борьбы с такими вирусами и научитесь противостоять вымогателям.

3.1. Блокировка компьютера — это результат действия СМС – вируса

Каждый день пользователи включают свои компьютеры и дожидаются загрузки рабочего стола с многочисленными ярлычками и любимой кнопкой "Пуск". Несколько секунд – и можно начинать работу. Данная последовательность действий стала настолько привычной, что появление сообщения о том, что компьютер заблокирован и вам необходимо отправить СМС на указанный номер, застанет врасплох даже самого продвинутого пользователя. Виной всему – вирусы-вымогатели, они же СМС-вирусы.

Специалисты назвали распространение СМС-вирусов настоящей эпидемией, учитывая масштаб бедствия. Согласно статистическим данным, представленным ведущими ИТ-компаниями, занимающимися антивирусными программами, СМС-вирусы поразили миллионы компьютеров. Пик заражения пришелся на начало 2010 года.

В настоящее время существует множество разновидностей данных вирусов. Но объединяет их одно – выманивание денег у растерянных пользователей. Расчет злоумышленников прост: в замешательстве многие пользователи выберут отправить СМС и получить заветный код. Ведь, на первый взгляд, это самый простой способ для решения всех проблем. Почему так делать не стоит, мы расскажем далее. А пока познакомимся с видами СМС-вирусов.

СМС-вирусы, блокирующие систему

Распознать данный вид вирусов очень просто. После загрузки появляется сообщение наподобие: "*Windows заблокирован. Для разблокировки необходимо отправить СМС с текстом XXX на номер YYY*". Не менее популярны уведомления об использовании нелицензионной копии Windows или о заражении системы вирусом. При этом не функционирует мышь, клавиатура работает в ограниченном режиме, а все попытки перезагрузить компьютер оказываются бесполезными. Некоторые вирусы могут проявить себя только после запуска любого приложения.

Волна этих вирусов захлестнула пользователей весной 2009 года, тогда же в Интернете появились конструкторы трояновблокировщиков в свободном доступе. Большинство вирусов данного типа были реализованы в виде .tmp-файлов. При инсталляции они прописывали свой код во временные папки и попадали в автозапуск. Первые трояны-блокировщики позволяли получить доступ к рабочему столу через средства специальных возможностей Windows, но последующие вариации оказались более проработанными и полностью блокировали доступ.

Самый распространенный СМС - вымогатель вирус **Trojan.Winlock** (рис. 3.1), относящийся к категории троянских вирусов. Попадая на компьютер, он полностью блокирует его работу за счет блокировки операционной системы.

О подобной модификации троянского вируса впервые рапортовала компания "Доктор Веб" в апреле 2009 года. Данный вирус ссылается на использование нелицензионной копии Windows и требует ввести регистрационный код. Получить код можно, отправив платное СМС с определенным текстом на указанный номер. Но сразу предупреждаем, что делать этого не стоит! Вирус устанавливает в систему дополнительную программу, блокирующую работу Windows. Вирус известен под такими названиями, как

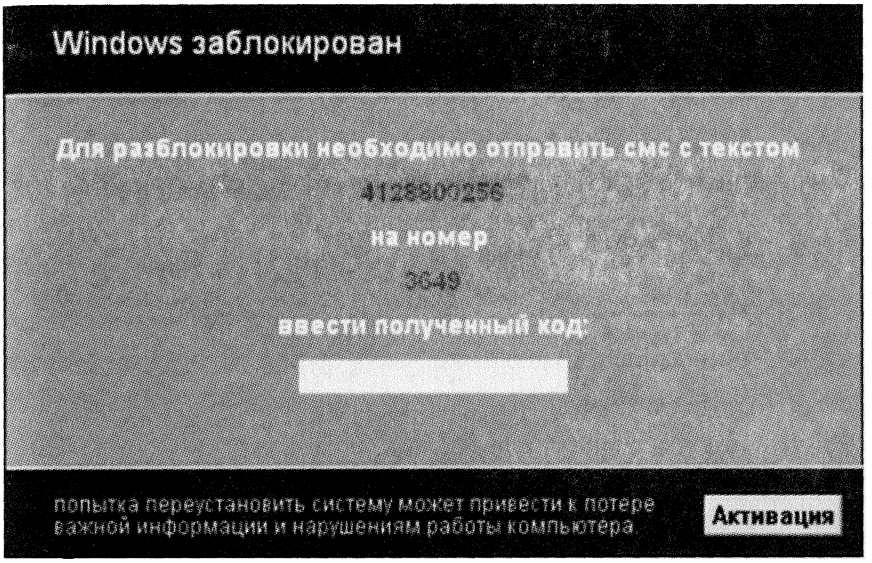


Рис. 3.1. Пример СМС-вируса Trojan.Winlock

Trojan.Winlock.19, Trojan.Winlock.origin, Trojan-Dropper.Win32.Blocker.a и Trojan-Ransom.Win32.Agent.af., Trj/SMSlock.A.

Более редкой разновидностью подобных СМС-вирусов является вирус, блокирующий загрузку компьютера. СМС-вирус вносит изменения в загрузочный сектор жесткого диска. Сообщение вируса появляется не на рабочем столе, а сразу после сообщения о возможном входе в Bios. Обычно пользователи видят красными буквами на черном фоне следующий текст "Компьютер заблокирован за просмотр запрещенного видео порнографического содержания с участием несовершеннолетних. Для разблокировки вам необходимо пополнить номер МТС 89854271477 на сумму 500 руб. Код Вы найдете на выданном терминалом чеке оплаты. Enter code:". Конечно, текст может варьироваться, а номера телефонов отличаться.

СМС-вирусы, блокирующие доступ к Интернету

Следующая категория СМС-вирусов - это вирусы, блокирующие работу не всей системы, а только доступ к Интернету (рис. 3.2). Троян – блокировщик Интернета появился в ноябре 2009 года. После включения компьютера и загрузки операционной системы пользователям всплывает окно поверх всех остальных окон с напоминанием о том, что лицензия на программный продукт Get Access (название может быть абсолютно другое) истекла. При этом вы можете и не использовать данное ПО.

Согласно предлагаемой инструкции пользователю необходимо в течение трех минут ввести код активации, получить который можно, отправив СМС на заданный номер. Если пользователь не успевает в отведенный срок ввести нужный код, следует перезагрузка системы, после которой происходит автоматическая

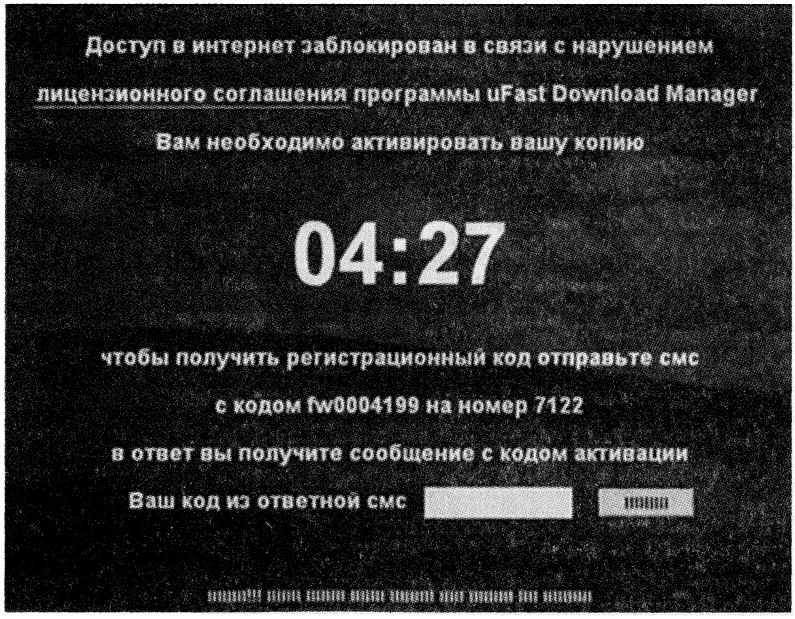


Рис. 3.2. Пример трояна-блокировщика

инсталляция вируса и его дальнейшая загрузка во всех режимах, включая безопасный. Параллельно СМС-вирус отключает средства восстановления системы (System recovery), и информационное окно вируса загружается уже поверх всех активных окон, препятствуя загрузке антивирусных программ.

Информационные баннеры в браузерах

СМС-вирусы данной категории не блокируют доступ к самой системе или отдельным ресурсам, а выводят информационные баннеры в браузерах поверх открытых сайтов. Баннеры содержат текстовую часть и окно для ввода кода деактивации, получить который можно по известному сценарию – отправив СМС на указанный номер. Казалось бы, не такая большая беда – ведь все работает. Но стоит посмотреть на содержание информационного баннера, как становится ясно, на что рассчитывали создатели вируса.

В окне баннера отображаются, как правило, изображения порнографического содержания. А ведь компьютером могут пользоваться и дети, и остальные домочадцы, и коллеги. Мало того, что они увидят подобные изображения, так еще и владельцу компьютера припишут путешествия по сайтам сомнительной тематики. Вряд ли кто добровольно захочет оказаться в щекотливой ситуации.

Вот вам и поток сообщений на получение кода деактивации. По этическим соображениям мы не будем демонстрировать примеры данных СМС-вирусов. С их идентификацией вы справитесь самостоятельно.

Информационные баннеры на рабочем столе

Результатом работы СМС-вируса могут быть не только информационные баннеры в браузерах, но и баннеры на рабочем столе компьютера. Чаще всего встречаются уже упомянутые выше баннеры с порнографическими изображениями или требованием установить "обновления" Windows. В первом случае вам опять предложат ввести код деактивации, а во втором – отправить СМС на заданный номер для получения кода обновления системы.

СМС-вирусы, блокирующие учетные записи

Вирусы данной категории блокируют ваши учетные записи на социальных сетях, форумах и других ресурсах. Вы набираете в адресной строке название любимого сайта, привычно вводите логин и пароль, а вместо загрузки персональной страницы видите сообщения различного содержания, но с единым смыслом – ваша учетная запись заблокирована, для активации записи...

Вы уже хорошо знаете, что предложат сделать мошенники – отправить СМС на заветный номер и получить код активации. Если вы не выполните указания в течение определенного промежутка времени, ваш аккаунт будет удален. Причины, по которым ваша учетная запись заблокирована, могут быть самыми разными – например, IP-адрес, с которого вы осуществляли вход на сайт, назван потенциально опасным из-за производимых с него спам-рассылок (рис. 3.3), или необходимо подтвердить принадлежность аккаунта с помощью мобильного телефона (рис. 3.4).

Основной механизм таких вирусов-вымогателей базируется на подмене настоящих страниц сайта на нужные злоумышленникам. Внешне кажется, что страница действительно с запрашиваемого сайта, на самом деле перед вами клон. Создатели сайта не имеют ничего общего с подобными инструкциями по активации учет-

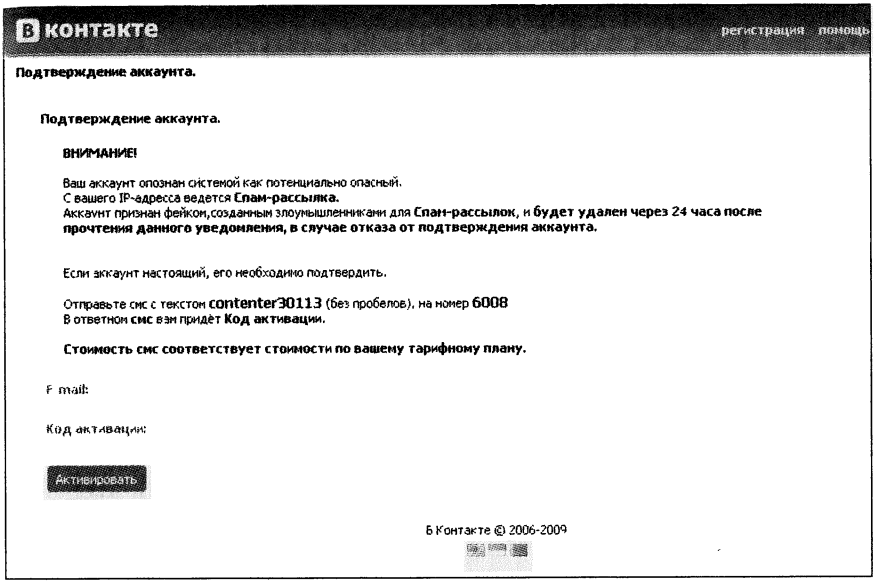


Рис. 3.3. СМС-вирус, блокирующий доступ в социальную сеть "Вконтакте"

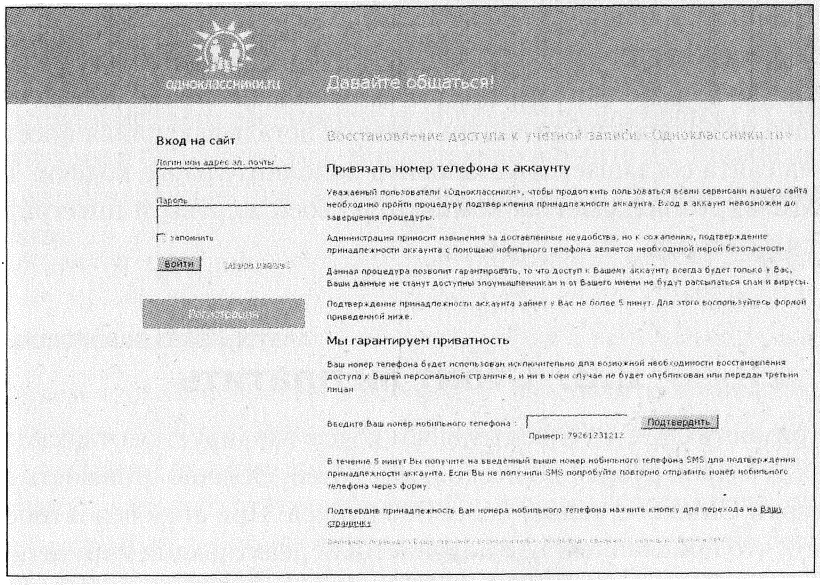


Рис. 3.4. СМС-вирус, блокирующий доступ в социальную сеть "Одноклассники"

ных записей. Ни в коем случае не отправляйте СМС, злоумышленники не только снимут с вашего телефона круглую сумму, но и получат в распоряжение ваши логин и пароль.

3.2. Как происходит заражение СМС-вирусом

Идеальная среда для распространения СМС - вируса (да и любого другого вируса) – это Интернет с его многочисленными социальными сетями, сайтами-обменниками, файловыми хранилищами, ICQ и другими средствами онлайн-взаимодействия. В таких условиях круговорот информации превращается в круговорот вредоносных программ.

Большинство заражений СМС-вирусами развивается по одному и тому же сценарию. Пользователям предлагается установить обновление для используемых на компьютере программ или плагинов для интернет-браузеров. Например, зайдя на сайт злоумышленников, пользователь видит окно с видеороликом. Поскольку видео не воспроизводится, ни о чем не догадывающийся посетитель сайта соглашается установить дополнительные кодеки. Так СМС-вирус попадает на компьютер своей жертвы и интегрируется в систему.

3.3. Стоит ли платить

Стоимость СМС со спасительным кодом варьируется от нескольких десятков рублей до нескольких сотен. Обычно стоимость отправки СМС составляет более 300 рублей. При этом вероятность того, что присланный код подойдет или деактивация вируса произойдет с первого раза, очень низкая.

Большинство вирусов-вымогателей после ввода полученного кода просят повторить процедуру получения кода или разблокируют компьютер, но только на время. Через некоторое время ситуация повторяется, и пользователь опять становится заложником вымогателей.

Отправка СМС – это настоящий подарок разработчикам вирусов-вымогателей. Известны случаи, когда с телефона пользователя списывалась не одна тысяча рублей или владелец телефона становился невольным подписчиком какой-либо услуги. Среди определенных категорий пользователей (дети, женщины, пожилые люди) процент отправивших СМС с целью получения кода превышает 70%. Неудивительно, что по данным СМИ доход от вирусов-вымогателей измеряется сотнями миллионов рублей.

Поэтому на вопрос, а стоит ли платить, ответ однозначный – нет!

3.4. Как снять блокировку самому

В этом разделе мы рассмотрим основные способы борьбы с СМС-вирусами и блокировками. Внимательно изучите их. Вполне возможно, что один из них поможет вам справиться с атакой мошенников.

Выключение компьютера

Начнем с самого простого способа – выключите компьютер и включите его через некоторое время. Конечно, надеяться на то, что проблема разрешится так просто, не стоит. Но, как известно, попытка – не пытка! Известно немало случаев, когда после таких элементарных действий вирус самоудалялся и больше не беспокоил пользователя. Если вам повезло и вирус вас покинул, не спешите расслабляться. Немедленно запустите на вашем компьюте-

ре любую антивирусную систему. Необходимо убедиться, что вирус не оставил после себя никаких следов.

Поиск вируса в списке процессов

Любой вирус, работающий на вашем компьютере, - это, прежде всего, запущенный процесс. В случае, когда вирус не заблокировал работу всей системы, можно попробовать найти вирус в списке активных процессов. Для этого выполните следующие действия:

1. Вызовите **Диспетчер задач**, нажав сочетание клавиш Ctrl + Alt + Delete или Ctrl + Shift + Esc. Перейдите на вкладку **Процессы**. Вы увидите список запущенных процессов (рис. 3.5).

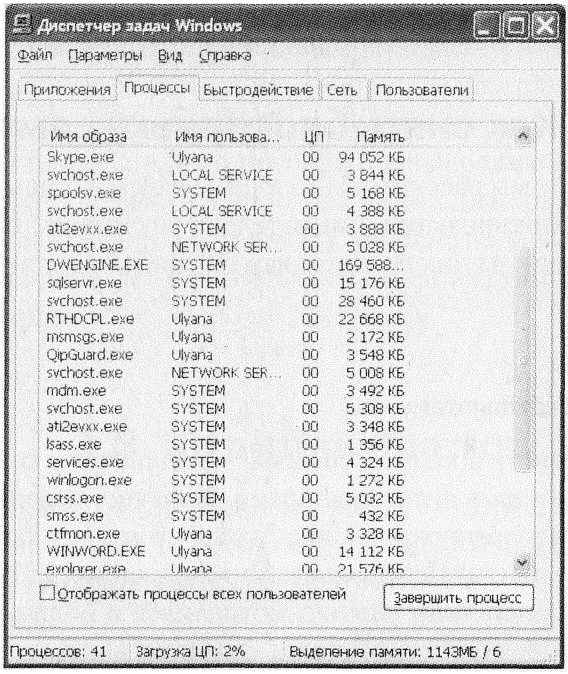


Рис. 3.5. Список запущенных на компьютере процессов

2. Внимательно изучите названия процессов. Определить вирус по названию процесса нелегко. Вирусам свойственно модифицировать свои имена. В подозрительную группу следует отнести процессы, названия которых состоят из одних цифр или произвольной комбинации символов. Так, процессы 12345678.exe или yetbh-02.exe с высокой долей вероятности окажутся вирусами.

3. Диспетчер задач позволяет завершать любой процесс. Если название процесса вызывает у вас сомнения – выделите его мышкой, нажмите на правую кнопку мышки. В появившемся меню выберите **Завершить процесс** (рис. 3.6).

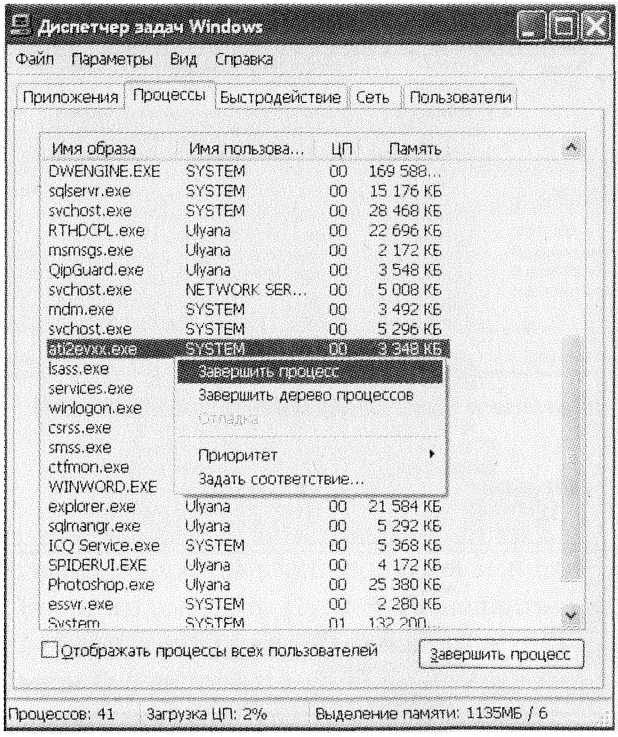


Рис. 3.6. Завершение подозрительного процесса

4. Если завершение процесса прошло успешно, не забудьте просканировать компьютер антивирусной программой, чтобы удалить все файлы вируса.

Большинство современных вирусов блокирует диспетчер задач. В этом случае на помощь могут прийти аналоги Диспетчера задач. Среди них наиболее известные:

- Process Explorer (рис. 3.7), позволяющий в режиме реального времени мониторить запущенные процессы. Как и Диспетчер задач, Process Explorer выводит информацию о загрузке процессора и позволяет закрывать процесс.

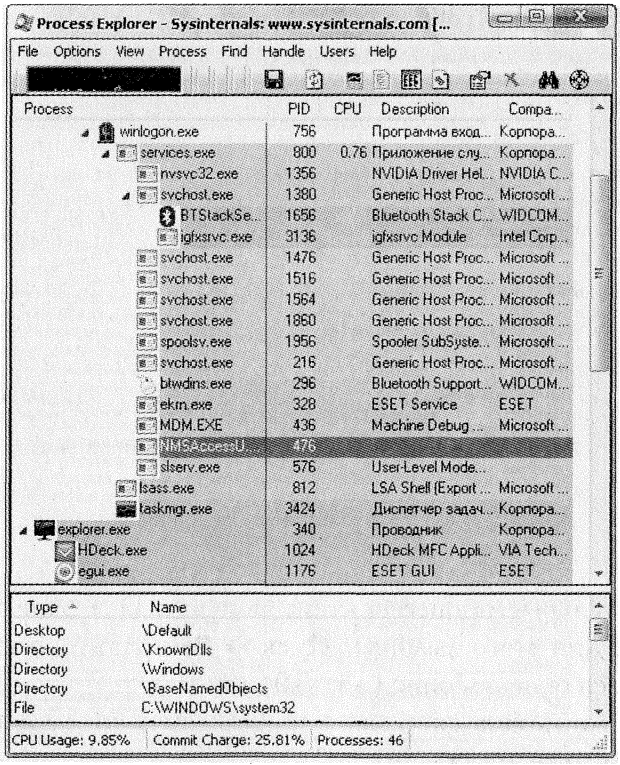


Рис. 3.7. Аналог Диспетчера задач - Process Explorer

- Process Lasso (рис. 3.8), ни в чем не уступающий предыдущему продукту.

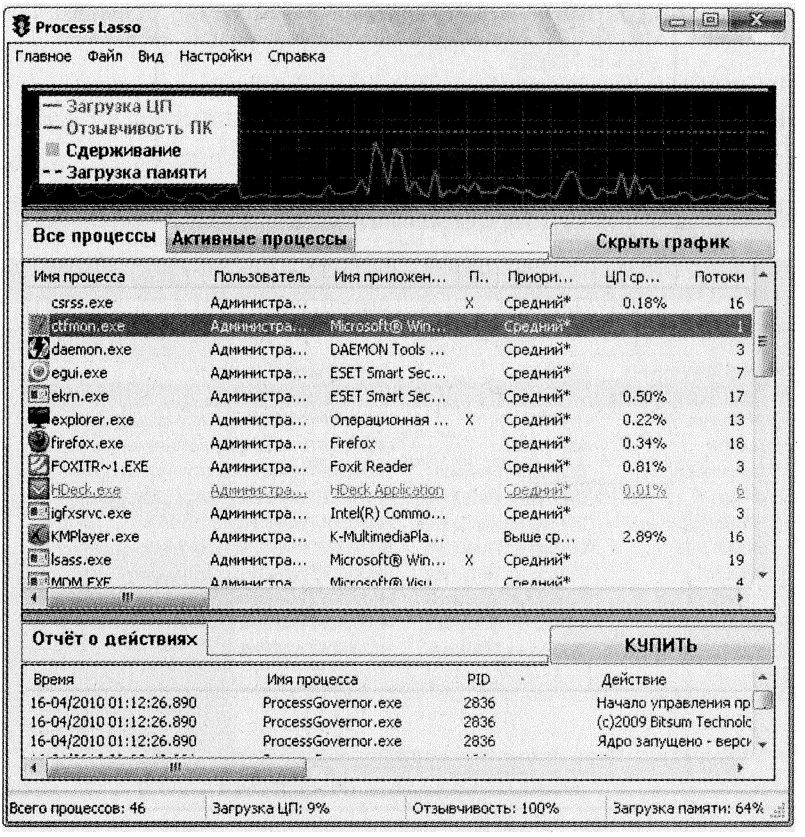


Рис. 3.8. Аналог Диспетчера задач - Process Lasso

Подозрительные процессы стоит поискать и в окне настройки системы. Для этого вызовите **Пуск ➔ Выполнить**. Введите в открывшемся окне msconfig (рис. 3.9) и нажмите OK. Откроется окно **Настройка системы**, в котором необходимо выбрать закладку **Автозагрузка** (рис. 3.10).

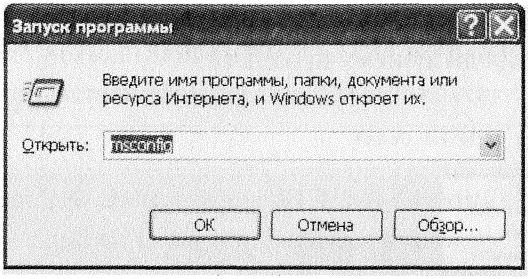


Рис. 3.9. Вызов окна настройки системы

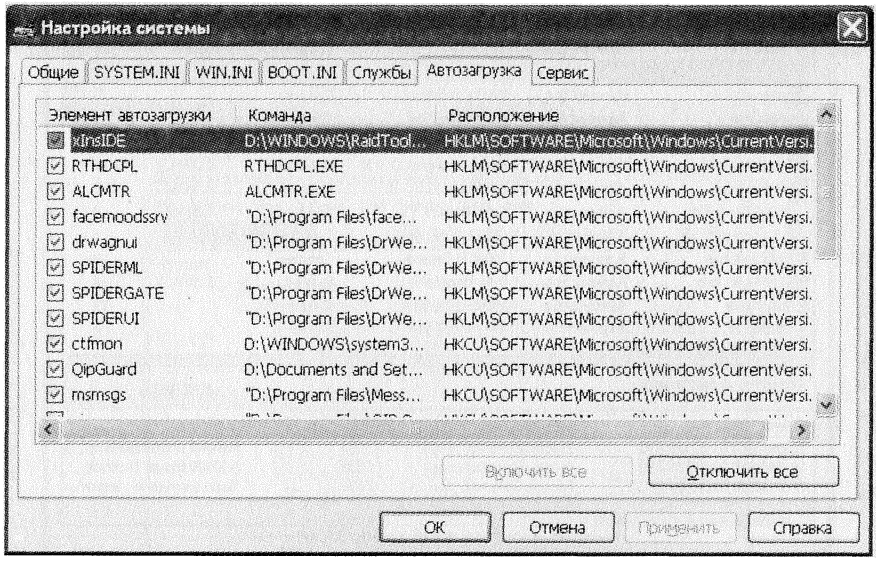


Рис. 3.10. Окно "Настройка системы"

В столбце **Команда** прописан полный путь к файлу. По нему вы сможете сориентироваться, где лежит сомнительный файл. В столбце **Элемент автозагрузки** можно снять флажок, убрав тем самым файл из автоматической загрузки. Так вы сможете отключить вирусный файл, и он не будет запускаться при загрузке Windows.

Поиск вируса в списке назначенных заданий

Некоторые разновидности СМС-вирусов могут оставить свои следы в списке назначенных заданий на вашем компьютере. Для доступа к списку назначенных заданий необходимо:

1. Нажать **Пуск → Все программы → Стандартные → Служебные → Назначенные задания** (рис. 3.11).

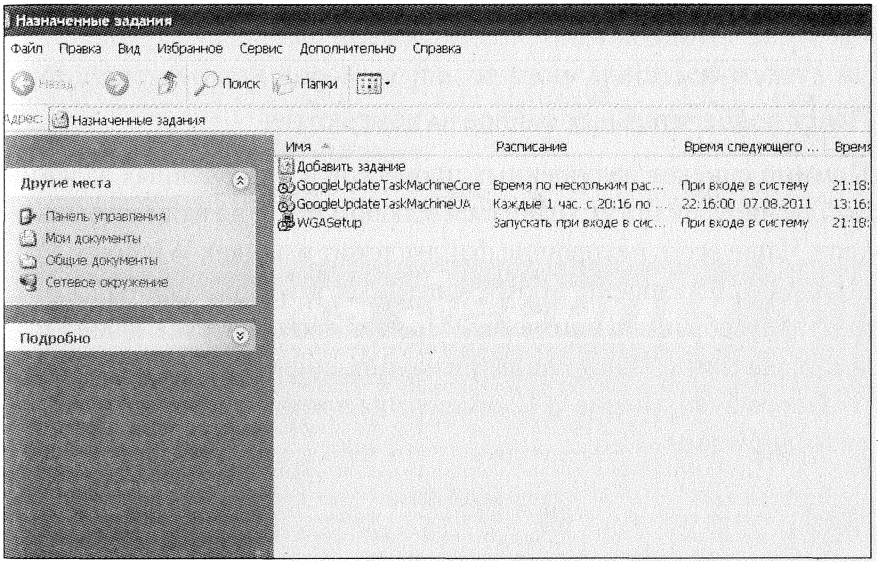


Рис. 3.11. Назначенные задания

2. Обычно в списке находится несколько заданий, если вы предварительно не меняли расписание. Обратите внимание, нет ли в списке задания с названием SYS CHECK. Зачастую именно так вирусы прописывают себя в список назначенных заданий.

3. Если вы обнаружили в списке задание SYS CHECK, кликните на него мышкой и посмотрите в открывшемся окне путь данного задания – адрес,

где лежат файлы. Удалите SYS CHECK из списка заданий и файлы по определенному ранее адресу.

4. После успешного удаления всех файлов не забудьте просканировать компьютер антивирусными программами.

К сожалению, данная проверка будет возможна только в том случае, если CMC-вирус не заблокировал работу с системой.

Поиск подозрительных файлов на компьютере

Помимо списков запущенных процессов и назначенных заданий файлы вирусов могут храниться в любом месте на вашем компьютере. Чаще всего нехорошие файлы лежат в папках Windows, Program Files, Documents and Settings/имя пользователя. На какие же файлы обращать внимания? Прежде всего, на .exe с невнятными названиями – состоящими из одних цифр или бессмысленного набора букв. На рис. 3.12 приведены примеры файлов, создаваемых вирусами.

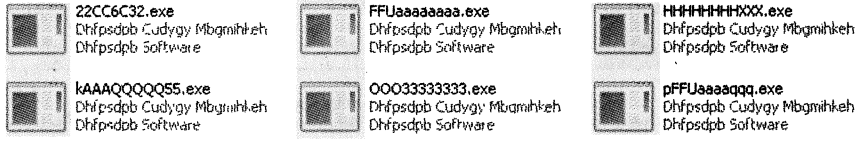


Рис. 3.12. Файлы, создаваемые вирусами

Допустим, что вы обнаружили подозрительный файл. Далее необходимо открыть свойства данного файла (кликнем правой кнопкой мышки по файлу и выбираем **Свойства**). Если в свойствах файла название не совпадает с названием самого файла или содержит непонятные надписи, то, скорее всего, перед вами файл вируса. Сомневаетесь и боитесь повредить нужный файл? Просто переименуйте этот файл, а затем перезагрузите компьютер.

Вирус исчез? Переименованный файл можно смело удалять – он был источником ваших проблем.

Подбор кода деактивации

Раз вирус-вымогатель требует ввести код, попробуем его подобрать. Подбор кода деактивации является самым распространенным решением в борьбе с СМС-вирусами! Данный метод отличается универсальностью: независимо от того, блокирует вирус доступ к системе или нет. Конечно́, не стоит пытаться угадать заветную комбинацию путем перебора клавиш на клавиатуре. Ни к чему хорошему это не приведет.

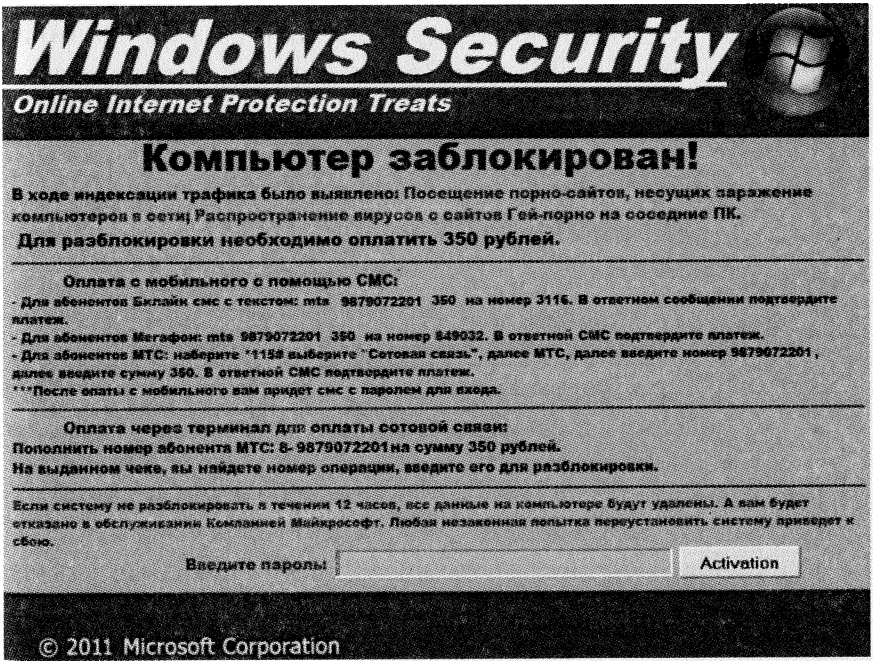


Рис. 3.13. Вирус-вымогатель

Если вы стали жертвой СМС-вируса, необходимо зайти с любого другого компьютера на один из сервисов деактивации вирусов в Интернете. Подавляющее большинство данных сервисов бесплатное. Для того чтобы получить код деактивации, необходимо указать текст сообщения и номер для отправки СМС. После чего будет подобран код, который необходимо ввести к себе на компьютер.

В помощь читателям мы приведем список кодов для деактивации наиболее популярных СМС-вирусов:

- Телефонный номер для отправки СМС: +7967... Возможные коды: 21122012, 66438899, 00052545#051999, b3s4lwYGaj1eh8owP0Al.

- Телефонный номер для отправки СМС: +7916... Возможные коды: 497499, 749092, 3397gj64, 647993099.

- Телефонный номер для отправки СМС: 2472. Возможные коды: 06159230, 49685761, 4479927959, 8694287294.

- Телефонный номер для отправки СМС: 3121. Возможные коды: j3qq4h, 1768684, 1234567, 2047692.

- Телефонный номер для отправки СМС: 4460. Возможные коды: gp223t90, drwee44x, 494332H64, 780976702.

- Телефонный номер для отправки СМС: 5121. Возможные коды: 2047692, 5114DJH, 780976702, 167443451.

- Телефонный номер для отправки СМС: 8353. Возможные коды: 2047692, 75112468, 1968845971, 2397672939.

Рассмотрим последовательность действий для конкретного случая. Например, вы увидели следующее сообщение (рис. 3.13) при блокировке компьютера.

Необходимо:

Зайти на сервис деактивации. На рис. 3.14 приведен соответствующий сервис от Dr.Web (http://www.drweb.com/unlocker/).

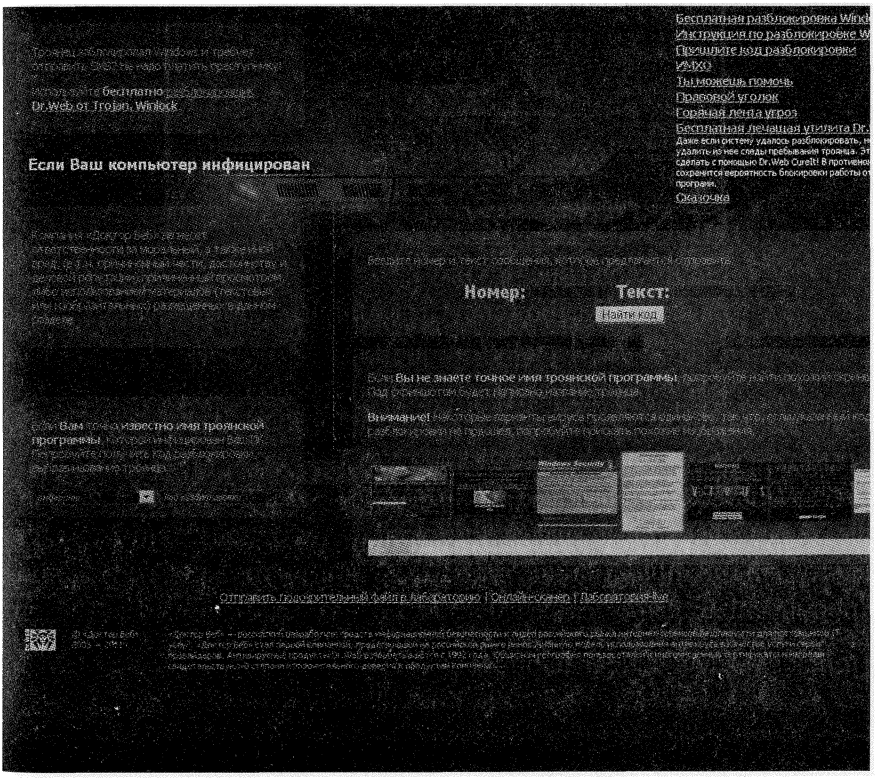


Рис. 3.14. Сервис деактивации от Dr.Web

1. Просмотрите скриншоты-образцы наиболее популярных вирусов. Если вы нашли подходящий, то щелкните на него два раза (рис. 3.15).

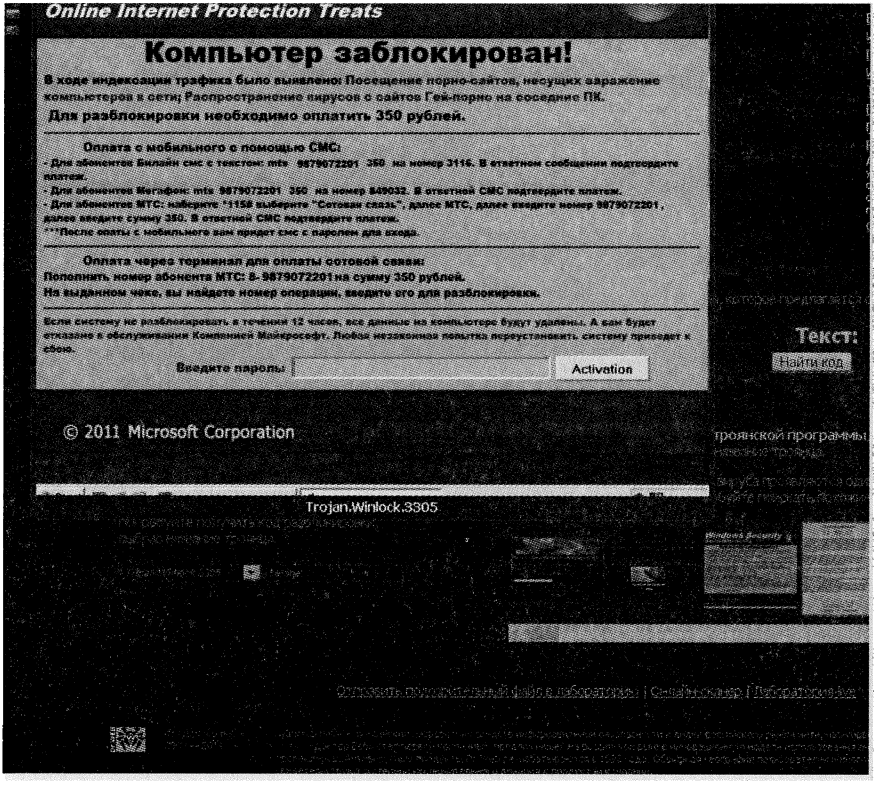


Рис. 3.15. Поиск похожего вируса

2. Вы увидите название вируса. В нашем случае речь идет о вирусе Trojan.Winlock.3305.

3. Теперь введите название вируса в соответствующем окне поиска вирусов (рис. 3.16), чтобы получить код.

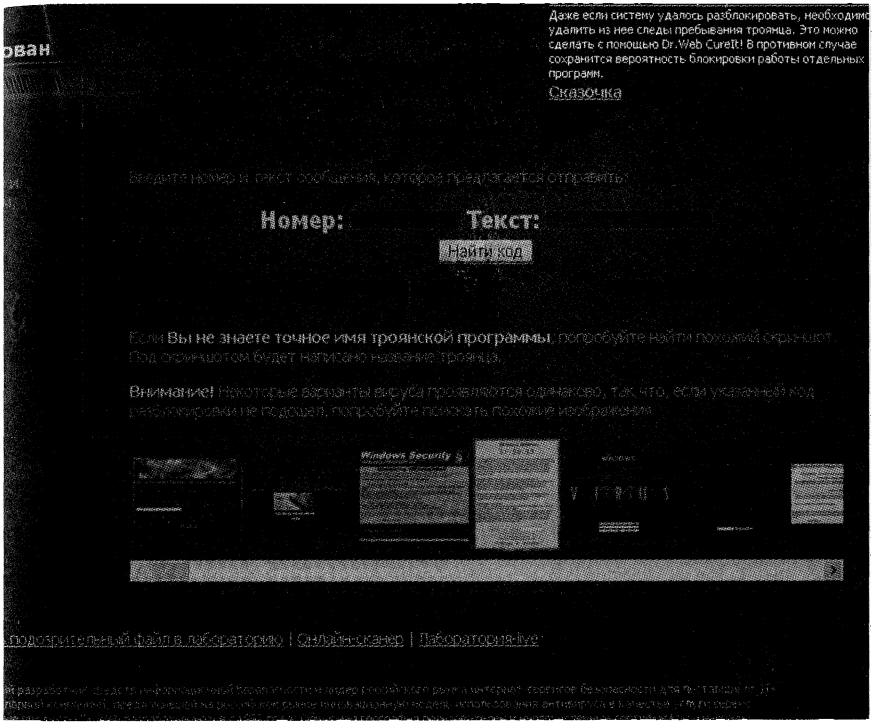


Рис. 3.16. Получение кода деактивации

4. Теперь полученный код необходимо ввести на ваш компьютер.

В том случае, когда ни один из представленных образцов вируса не подошел, необходимо ввести номер телефона, на который просят отправить сообщение, а также текст самого сообщения. Так, для вируса, выводящего сообщение на рис. 3.17, следует ввести в поле Номер: 3649, в поле Текст: 4128800256, как показано на рис. 3.18. Теперь нажмите на кнопку OK, чтобы получить код (рис. 3.19).

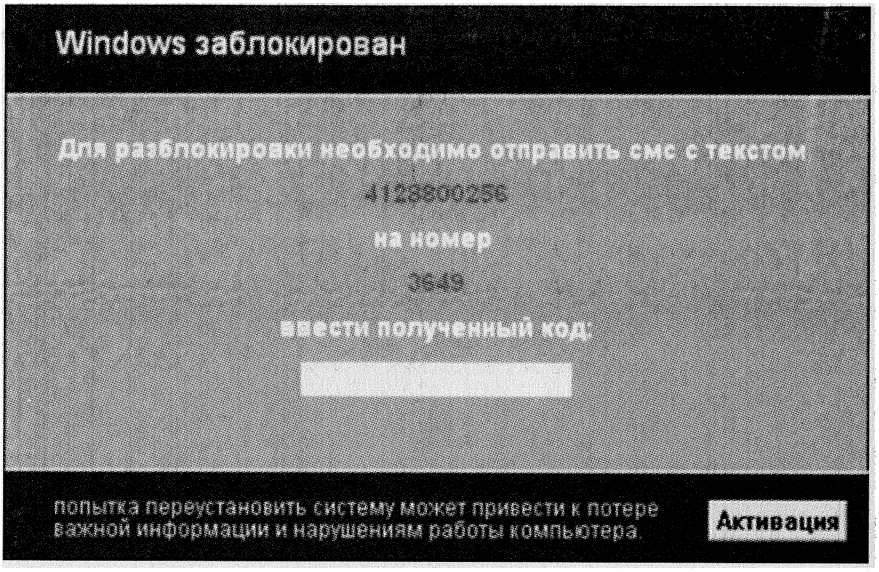


Рис. 3.17. Вирус-вымогатель

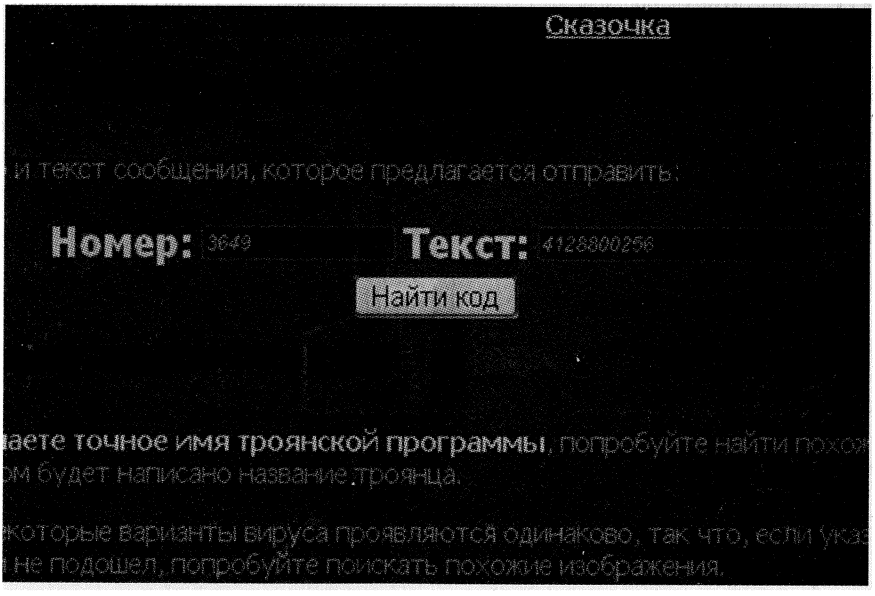


Рис. 3.18. Ввод данных о вирусе-вымогателе

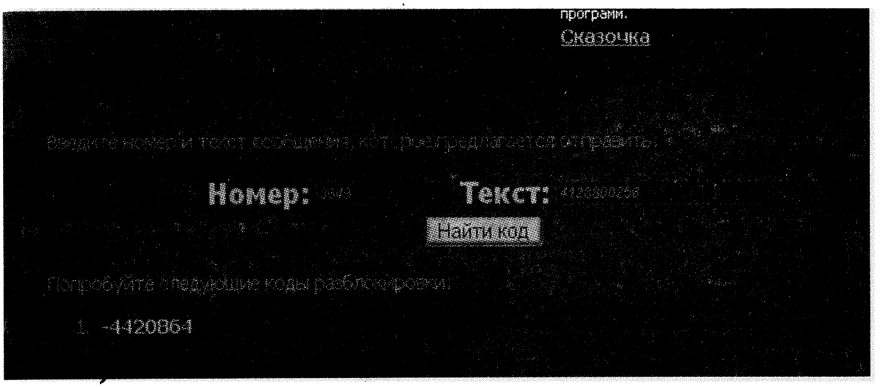


Рис. 3.19. Полученный код деактивации

Все сервисы деактивации работают на основе подбора кода, который действует для конкретного вируса. Вот почему рекомендуется использовать сразу несколько сервисов для подбора кода. Помимо сервиса от Dr.Web вы можете воспользоваться:

Сервисом от лаборатории Касперского (рис. 3.20), доступным по адресу http://support.kaspersky.ru/viruses/deblocker.

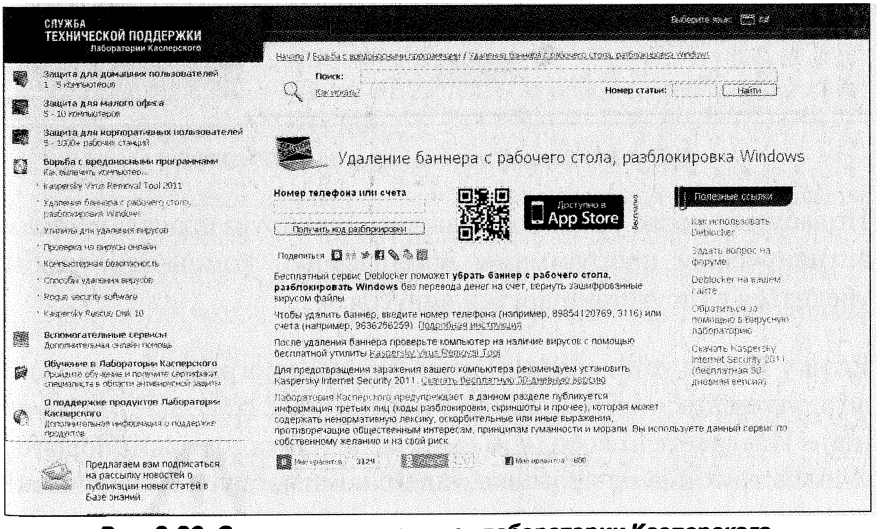


Рис. 3.20. Сервис деактивации от лаборатории Касперского

Сервисом от ESET NOD32 (рис. 3.21), доступным по адресу http://www.esetnod32.ru/.support/winlock/

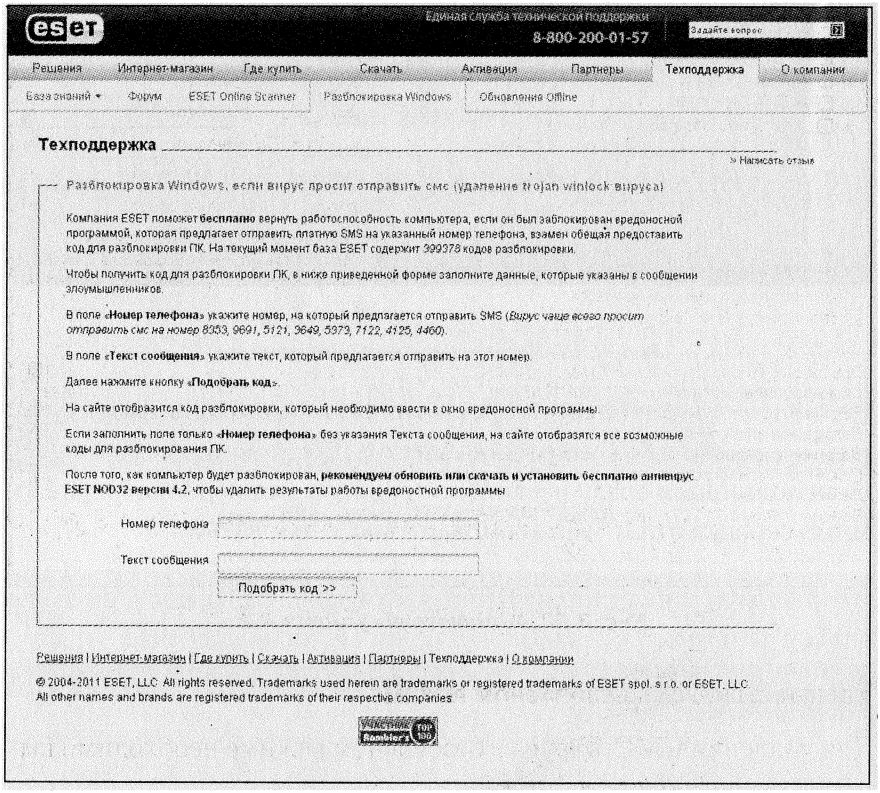


Рис. 3.21. Сервис деактивации от ESET NOD32

Не забудьте после успешной деактивации вируса просканировать антивирусным программным обеспечением компьютер, чтобы убедиться в отсутствии других вирусов.

Если у Вас не установлены антивирусные программы, то можно воспользоваться антивирусной утилитой AVZ (рис. 3.22), доступной в Интернете в свободном доступе. Утилита содержит пошаговую инструкцию по проверке вашего компьютера на наличие вирусов.

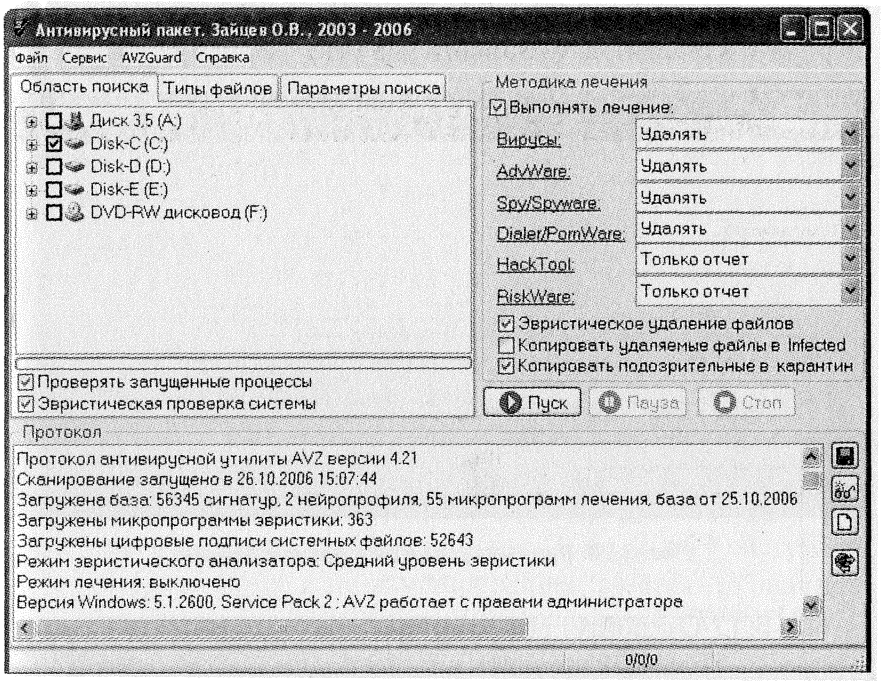


Рис. 3.22. Антивирусная утилита AVZ

Удаление вируса в безопасном режиме

Для удаления CMC-вируса в безопасном режиме необходимо выполнить следующие действия:

1. Первым делом перезагрузите компьютер в безопасном режиме. Для этого сразу после начала перезагрузки несколько раз нажмите на «F8». В появившихся вариантах загрузки (рис. 3.23) выберите пункт **Безопасный режим**.

2. Найдите на компьютере файлы blocker.exe, blocker.bin и удалите их.

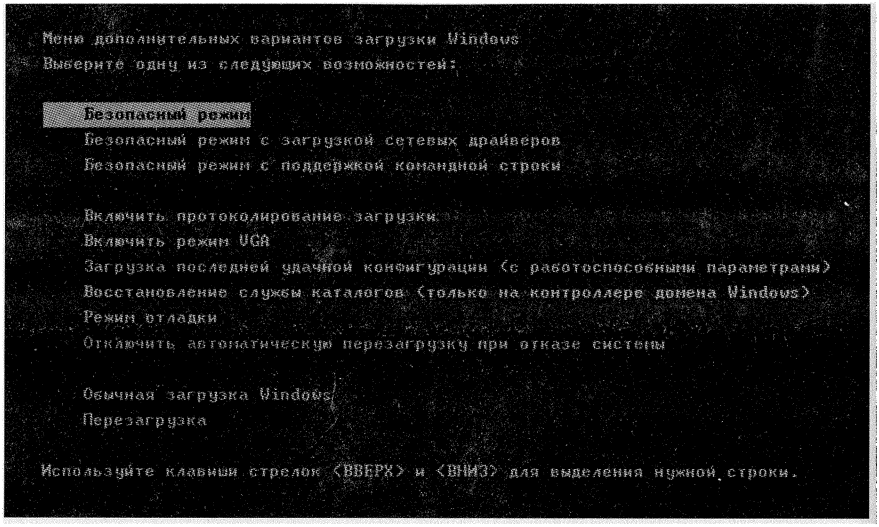


Рис. 3.23. Перезагрузка в безопасном режиме

3. Откройте редактор реестра (рис. 3.24): нажмите **Пуск➔Выполнить** и в появившемся окне введите команду regedit (рис. 3.25).

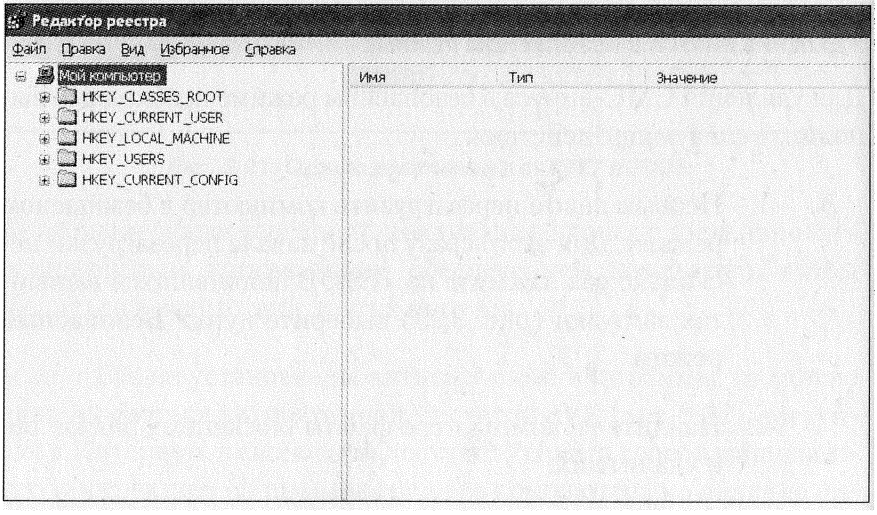


Рис. 3.24. Редактор реестра

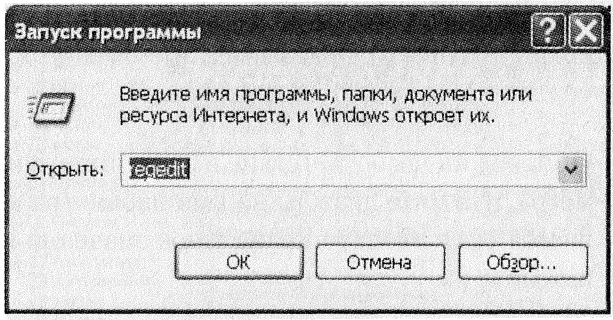


Рис. 3.25. Вызов редактора реестра

4. Последовательно спуститесь по уровням:

HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/WindowsNT/CurrentVersion/ Winlogon и посмотрите на значение параметра userinit (рис. 3.26). Если в систему не вторгся вирус и не изменил записи реестра, то значение параметра userinit должно быть равно C:/WINDOWS/

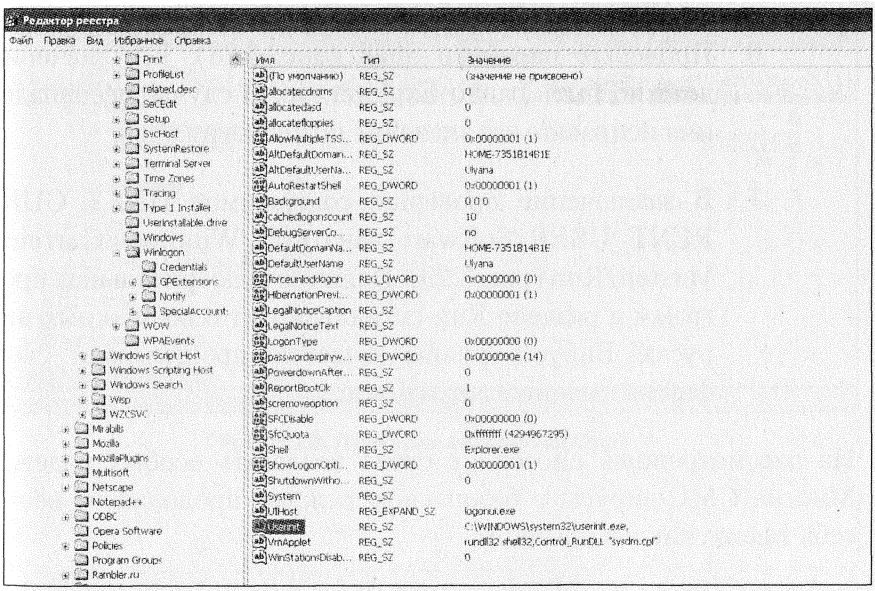


Рис. 3.26. Проверка параметра userinit

system32/userinit.exe. А вот путь после C:/WINDOWS/system32/userinit.exe показывает, где именно таится файл вируса. Его-то и нужно ликвидировать.

5. Обнаружив несоответствие в значениях данного параметра, нажмите дважды на имя параметра и в появившемся окне введите правильное значение (рис. 3.27), нажмите на OK.

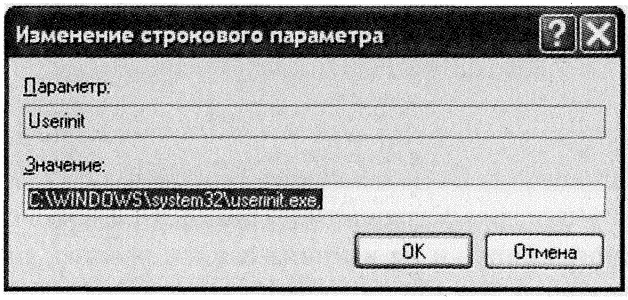


Рис. 3.27. Корректировка параметра userinit

6. Проверьте параметр Shell (рис. 3.28). Его значение должно быть равно Explorer.exe. В случае несовпадения исправьте его значение по аналогии с п.5.

7. В заключение проверьте содержимое HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Run (рис. 3.29). Наличие подозрительных программ в разделе Run сигнализирует о возможных вирусах. Вирусы-трояны зачастую прописывают свои файлы именно в автозапуск.

На рассмотренный способ не стоит возлагать особых надежд. Многие СМС-вирусы в безопасном режиме продолжают вести себя так же, как и в обычном.

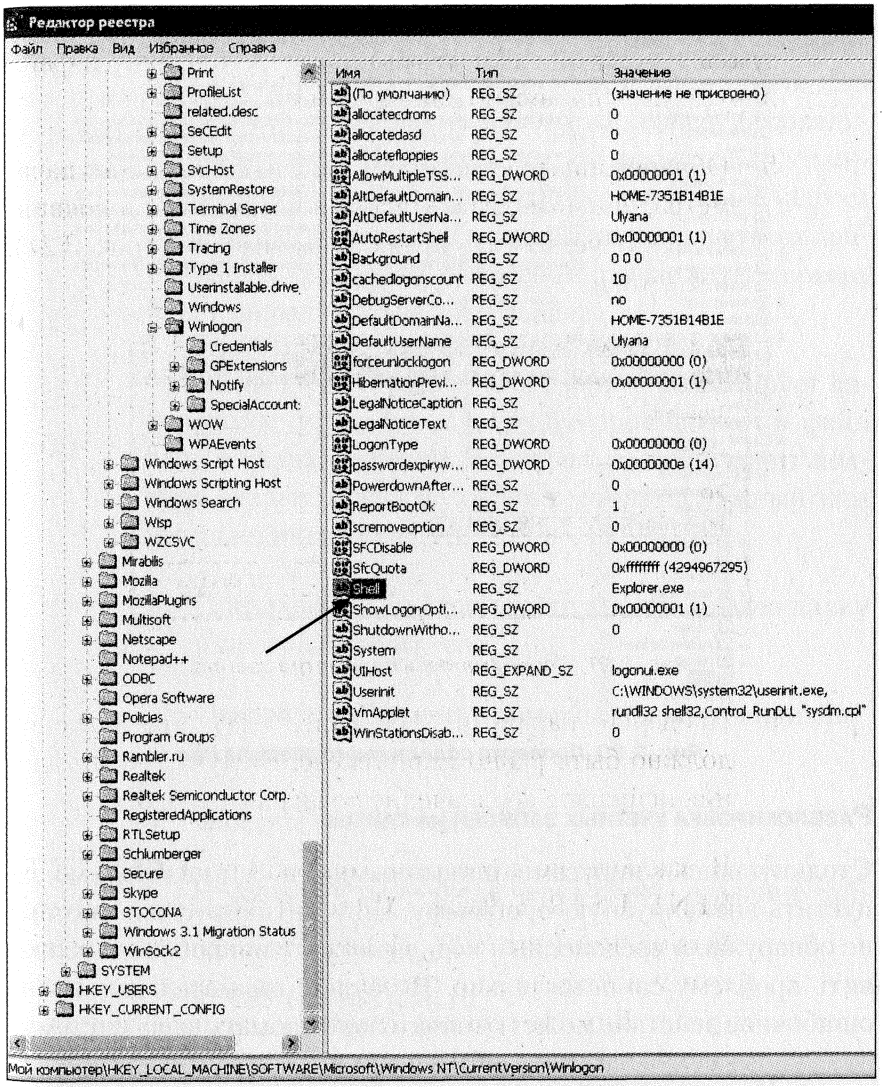


Рис. 3.28. Проверка параметра Shell

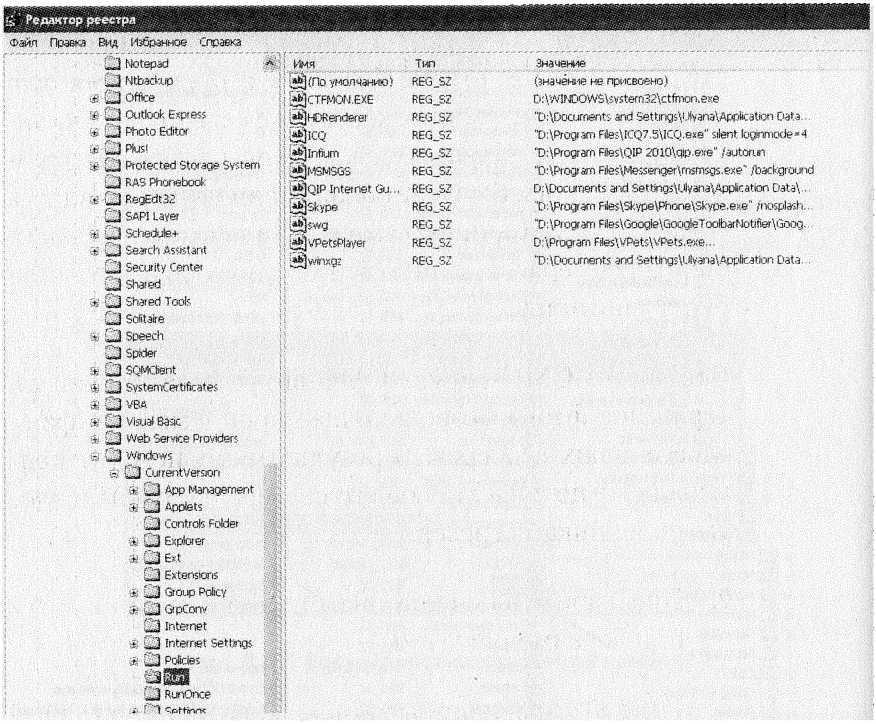


Рис. 3.29. Проверка содержимого раздела Run

Разблокировка учетных записей на сайтах

Столкнувшись с вирусами, описанными в п. 3.1, необходимо запустить антивирусную программу. Если антивирусная система не обнаружила вредоносный код, вы можете попробовать исправить проблему самостоятельно. Но будьте внимательны, любое ошибочное действие может окончательно сломать вашу систему!

Итак, ваши действия:

1. Найдите файл hosts, доступный по следующему пути: <диск, на котором установлена ваша система:\WINDOWS\system32\drivers\etc.

Зачем нужен этот файл? Вы набираете доменное имя сайта в адресной строке браузера, а в это время ваш компьютер определяет, к какому же серверу необходимо обратиться. Первым делом проверяется содержимое файла hosts. В случае обнаружения в нем IP-адреса сервера для указанного вами имени используется данный адрес сервера. В противном случае адрес сервера будет запрашиваться у провайдера.

Что делает СМС-вирус? СМС-вирус редактирует содержимое файла hosts, а точнее прописывает в файл адреса своих серверов. В результате происходит подмена реально существующего сервера на нужный злоумышленникам серевер.

2. Предварительно скопируйте файл в другую папку или переименуйте его.

3. Откройте файл hosts с помощью блокнота или иного редактора.

4. Найдите строки вида:

   IP-адрес (четыре числа через точку) название сайта. Например:

   91.189.113.145 mail.ru

   91.189.113.145 www.mail.ru

   91.189.113.145 www.google.ru

   91.189.113.145 google.ru

   91.189.113.145 www.vkontakte.ru

91.189.113.145 vkontakte.ru

91.189.113.145 www.odnoklasniki.ru

91.189.113.145 odnoklasniki.ru

Исключение составляет строка: 127.0.0.1 (или другой адрес) localhost. Ее ни в коем случае нельзя удалять.

5. Удалите найденные строки (кроме строки localhost).

6. Сохраните файл.

7. Закройте браузер и вновь попытайтесь войти на сайт, на котором был замечен СМС-вирус. Проблема должна быть устранена.

Проверка жесткого диска на другом компьютере

Данным способом смогут воспользоваться не просто опытные пользователи, но и те, кто хорошо знаком с аппаратной составляющей компьютеров. Если вы знаете, что такое винчестер (жесткий диск) и как его можно снять, а ваш системный блок не защищен магазинной пломбой, можно попробовать снять жесткий диск и подключить его к любому другому незараженному компьютеру. Далее необходимо проверить винчестер с помощью антивирусной системы.

Метод, безусловно, на любителя, но имеет право на существование.

Загрузка с LIVE CD

Если против СМС-вируса оказываются бессильны все рассмотренные выше методы, не стоит отчаиваться. Можно попробовать удалить СМС-вирус, воспользовавшись специальной программой RegEdit и загрузив операционную систему с Live CD.

Live CD (от англ. CD Live Distro – "живой" компакт-диск) - это операционная система, загрузка которой осуществляется с загрузочного диска CD. Загрузка может быть выполнена и с иного съемного носителя (DVD, USB-накопитель), соответственно речь пойдет уже о Live DVD или Live USB.

Использование Live-носителей позволяет избежать длительной установки операционной системы в постоянную память компьютера. Весь процесс займет не больше нескольких минут.

Обычно вирусы-блокировщики искажают параметры реестра, а это в свою очередь препятствует нормальной загрузке Windows. Поэтому для удаления вирусов необходимо восстановить ключи реестра и физически удалить исполняемые файлы вируса, прописанные в измененных параметрах.

Алгоритм работы будет следующим:

1. Скачайте из Интернета с другого компьютера образ Live CD, например ERD Commander, и запишите образ на любой съемный носитель.

2. Загрузите свой компьютер с Live CD, записанного на съемном носителе.

3. Вызовите редактирование реестра. Нажмите **Пуск →Выполнить** и в появившемся окне введите команду regedit (рис. 3.30), а затем нажмите OK.

4. В открывшемся окне редактора реестра раскройте ветвь HKEY_USERS (рис. 3.30). Сделать это необходимо для того, чтобы отредактировать реестр именно вашего компьютера, а не Live CD.

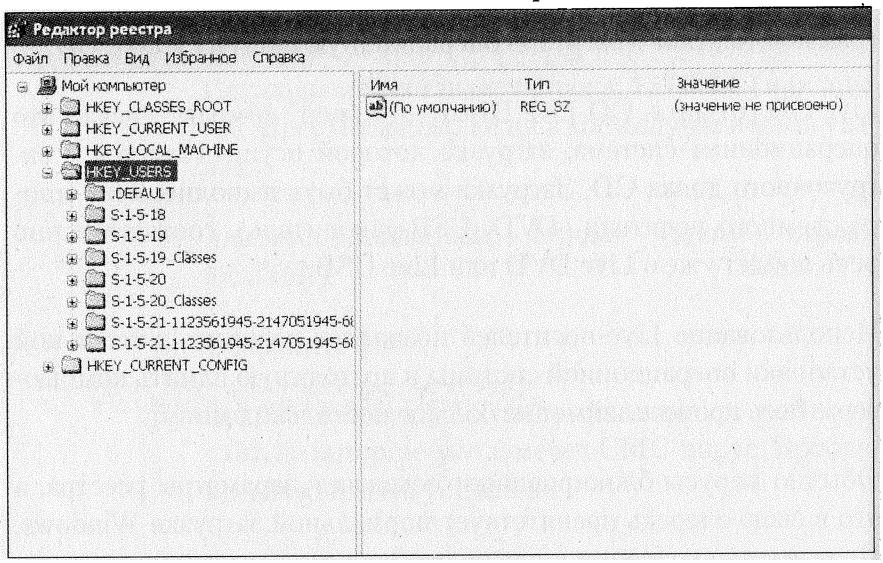


Рис. 3.30. Редактор реестра. Выбор нужной ветви

5. Выберите **Файл ➔ Загрузить куст** (рис. 3.31).

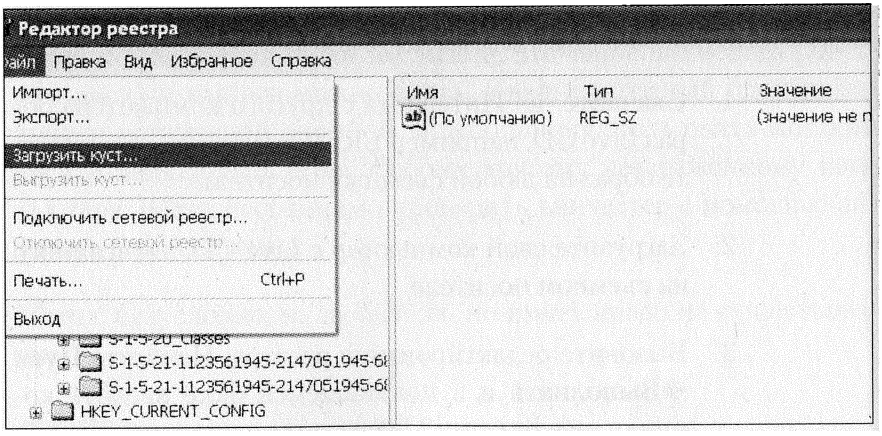


Рис. 3.31. Редактор реестра. Работа с меню

6. Дождитесь, когда откроется окно (рис. 3.32), и перейдите в директорию [диск, на котором установлена Windows]\Windows\system 32\config\. Далее выбор ветви зависит от того, какую ветвь реестра вы желаете изменить. Так, для редактирования ветви HKLM\SOFTWARE необходимо в папке config выбрать куст SOFTWARE. Затем нажмите на Открыть.

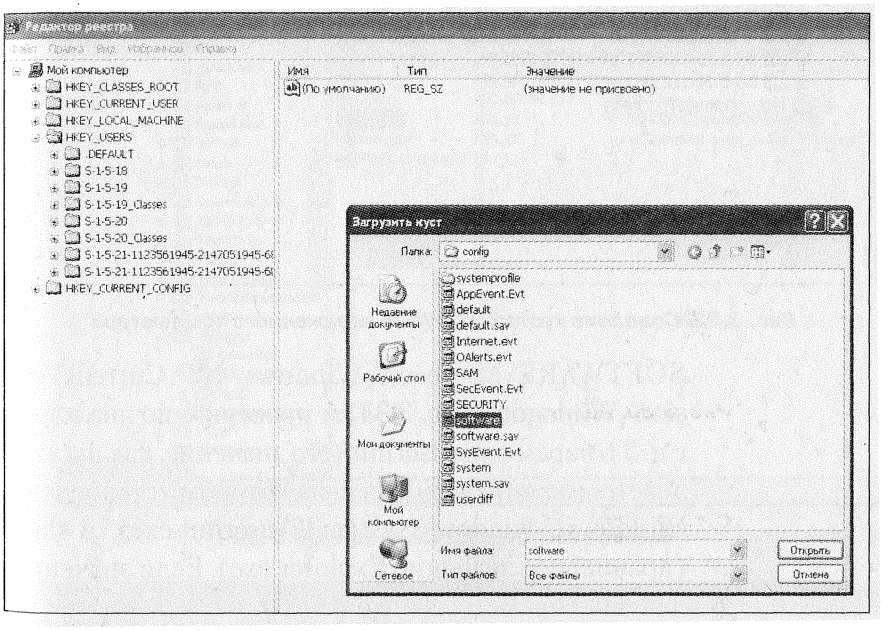


Рис. 3.32. Выбор ветви редактирования в реестре

7. Введите название для нового раздела и нажмите ОК. В HKEY_USERS появилась новая ветвь – куст SOFTWARE зараженного компьютера (рис. 3.33).

8. Теперь скорректируем параметры реестра. Откройте в реестре ветвь HKEY_LOCAL_MACHINE\

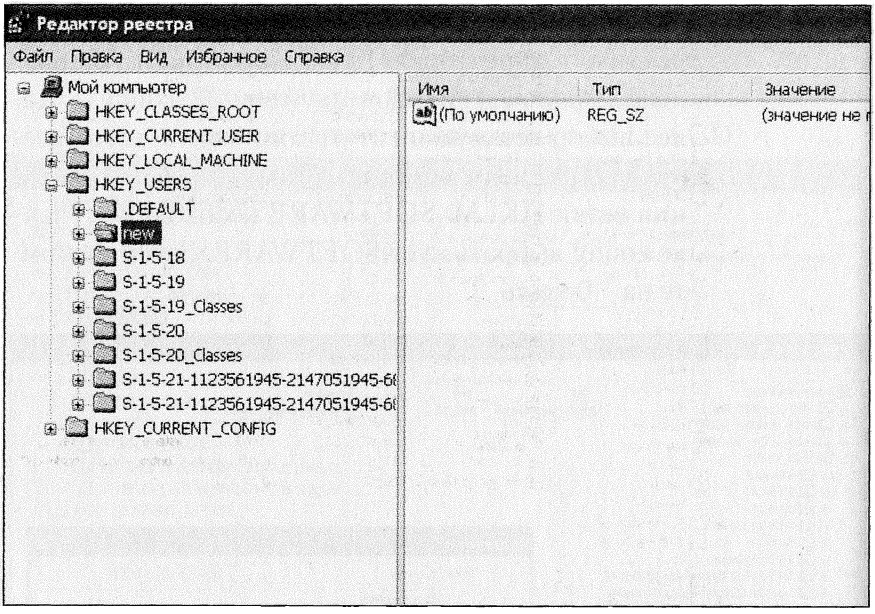


Рис. 3.33. Создание куста SOFTWARE зараженного компьютера

SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon (рис. 3.33) и проверьте по аналогии с п. 3.6 параметры userinit (его значение, как вы уже знаете, должно быть [диск, на котором установлена Windows]:\windows\system32\userinit.exe) и shell (правильное значение Explorer.exe). Если значения данных параметров отличаются, то следует внести исправления.

9. После редактирования параметров реестра следует выгрузить куст. Для этого выделяем созданную ранее ветвь (new на рис. 3.34), нажимаем **Файл → Выгрузить куст** (рис. 3.35) и нажимаем ОК.

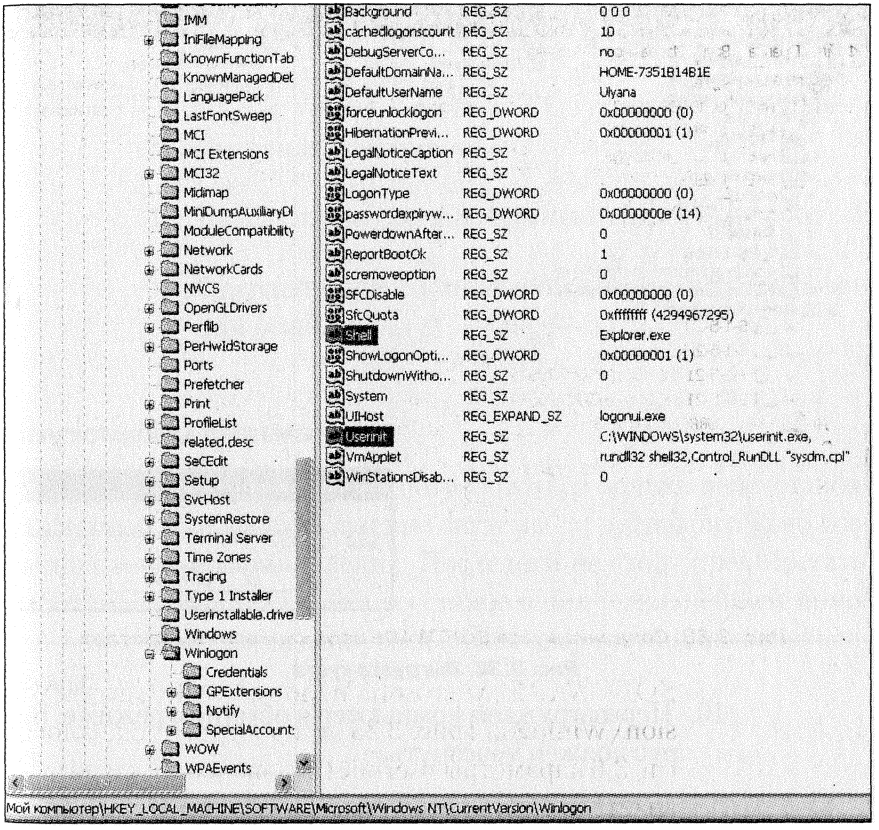


Рис. 3.34. Проверка параметров реестра

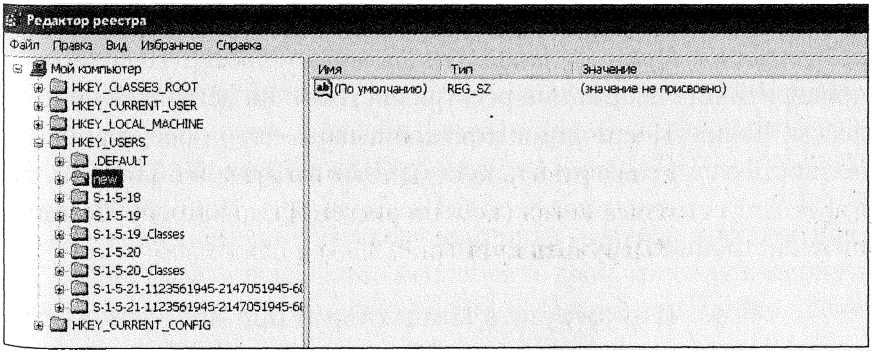


Рисунок 3.35. Выделение созданной ранее ветви

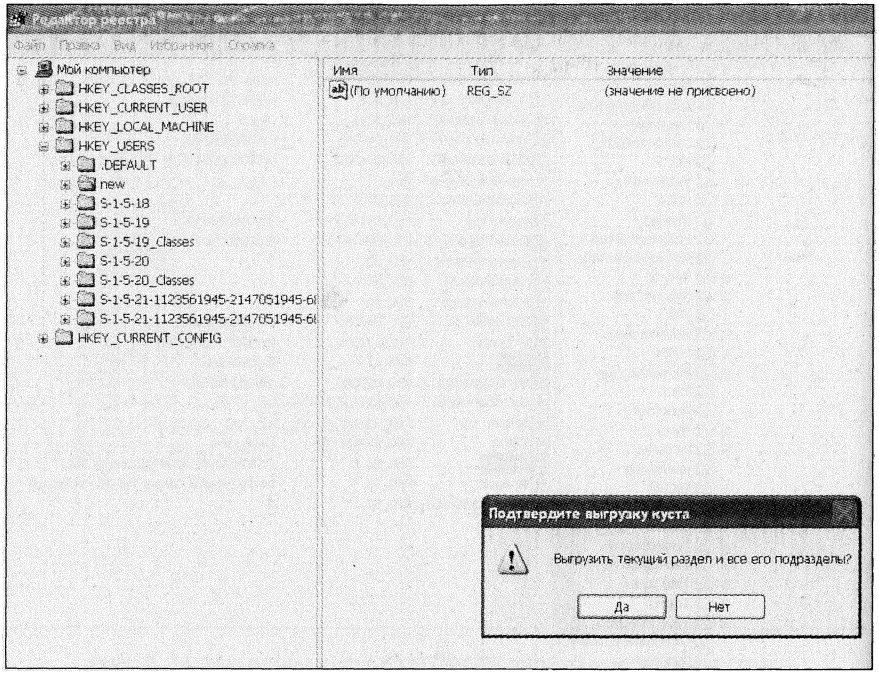


Рис. 3.36. Выгрузка куста

10. Перезагружаем компьютер в обычном режиме. Вирус должен исчезнуть.

Редактирование настроек BIOS

Столкнувшись с CMC-вирусом, блокирующим загрузку компьютера, пользователи находятся в замешательстве. Невозможно проверить ни содержание реестра системы, ни запущенные процессы. Кажется, что единственный выход – это переустановить полностью систему или воспользоваться загрузкой с Live CD. Но в арсенале есть еще одна скрытая возможность. Попробуйте изменить настройки BIOS. Для этого:

1. Перезагрузите компьютер и при включении компьютера нажмите F2 или кнопку “Del”.

2. Измените системную дату на несколько месяцев вперед (например, если сейчас август, установите декабрь).

3. Сохраните настройки.

4. Перезагрузите заново компьютер.

5. Операционная система должна загрузиться в обычном режиме.

Переустановка системы

В некоторых случаях может потребоваться полная переустановка системы или восстановление системы по предварительно созданной точке восстановления. Последней не стоит пренебрегать. Заботливо созданная точка восстановления в дальнейшем поможет без особого труда вернуться к рабочему состоянию вашей системы.

3.5. Как не заразиться СМС-вирусом

Всем известно, что профилактика лучше всякого лечения. Конечно, с вирусами можно бороться, и большинство из них будет благополучно удалено при грамотном подходе. Но лишние проблемы никому не нужны! Что делать, если вы подхватили СМС-вирус, вы уже знаете. А теперь погорим о том, как вести себя, чтобы уберечься от вредоносных атак.

Самая надежная защита от компьютерных вирусов, которую вряд ли можно будет превзойти, - выключить компьютер и выдернуть его из розетки. Но сомневаемся, что найдутся желающие после-

довать такому совету. Поэтому приведем менее надежные, но зато жизненные рекомендации.

Итак, **правило номер один** - установите на своем компьютере антивирусную систему. Не стоит экономить и, если позволяют средства, приобретите полноценный лицензионный продукт, с постоянно обновляющимися базами и развитыми механизмами защиты. Если покупка лицензионной системы для вас затруднительна, можно воспользоваться любым бесплатным антивирусным комплексом. Конечно, бесплатные антивирусники, как правило, предоставляют меньшие возможности, нежели платные аналоги. Но лучше иметь хоть какую-то защиту, чем не иметь ее вообще. Антивирусные системы – это не панацея, а повышение уровня безопасности вашего компьютера. "Продвинутый" вирус всегда найдет обходные пути, а вот уже известный и не раз встречающийся вирус будет отслежен и беспощадно удален.

Правило второе – не посещайте сайты сомнительного содержания. Как показывает практика, основной рассадник СМС-вирусов сосредоточен на сайтах, содержащих порнографический материал, и на ресурсах, предназначенных для просмотра и обмена аудио- и видеоинформацией. Не меньше СМС-вирусов и в социальных сетях. Но совет избегать таких сайтов из области фантастики. Наслаждайтесь общением с друзьями и просмотром фотографий, но только с включенной антивирусной системой.

Правило третье является логическим продолжением предыдущего пункта. Не выходите в Интернет с незапущенным антивирусником.

Правило четвертое призывает пользоваться только надежными и проверенными источниками информации. Вирусы могут попасть в компьютер не только через Интернет, но и с дисков, флешек.

Правило пятое – будьте бдительны! Зачастую пользователи становятся жертвой СМС-вирусов по причине своей же собственной беспечности. Если вы работаете в Интернете и неожиданно получаете предложение на установку какого-либо обновления, сулящего вам привлекательные возможности, хорошенько подумайте, чем может закончиться такая установка. Не верьте и предложениям посмотреть свои фотографии, размещенные на каком-либо сайте, или узнать переписку своих друзей. Не доверяйте и сомнительным спонтанным сообщениям, приходящим в социальные сети от ваших же друзей. Зачастую ваши друзья и не подозревают, что отправили вам такие послания. И даже если ваш друг сообщает вам о том, что от вас приходит спам, и заботливо предлагает установить антивирусную систему, доступную по ссылке, не торопитесь выполнять предложенные действия. Не принимайте файлы от неизвестных отправителей через icq, qip и прочие агенты. Все это может оказаться проделками мошенников, изобретательность которых растет с каждым днем. Остап Бендер мог бы гордиться находчивостью разработчиков современных вирусов.

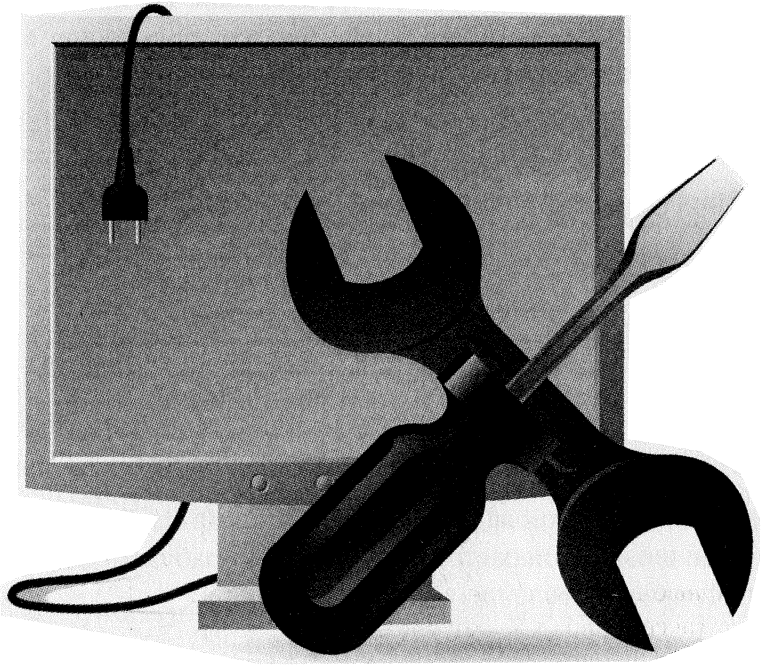
Правило шестое – не используйте Internet Explorer 6 для работы в Интернете. Многие жертвы компьютерных вирусов уверяют, что заразились именно через Internet Explorer 6. Скачайте Internet Explorer 8 или используйте любой другой браузер. Не хотим обижать самый распространенный браузер, но опытные IT-специалисты не используют сами и не рекомендуют другим Internet Explorer.

Правило седьмое адресовано счастливым обладателям честно купленной лицензионной системы Windows – не забудьте включить автоматическое обновление.

Обещаем, что выполнение этих незамысловатых правил значительно сэкономит ваши нервные клетки и убережет от многих неприятных приключений.

ГЛАВА 4.

КОМПЬЮТЕРНЫЕ ВИРУСЫ И ПРОБЛЕМЫ, СВЯЗАННЫЕ С НИМИ. КАК ВИРУСЫ МОГУТ ПОПАСТЬ НА КОМПЬЮТЕР?



4.1. Компьютерные вирусы

Основой данного описания послужили материалы Википедии (http://ru.wikipedia.org).

Классификация

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы по поражаемым объектам (файловые вирусы, загрузочные вирусы, скриптовые вирусы, сетевые черви), по поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unix, GNU/Linux, Java и другие), по технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы), по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, скриптовый язык и др.).

По способу заражения файловые вирусы (вирусы, внедряющие свой код в исполняемые файлы: командные файлы, программы, драйве-

ры, исходный код программ и др.) разделяют на перезаписывающие, паразитические, вирусы-звенья, вирусы-черви, компаньон-вирусы, а также вирусы, поражающие исходные тексты программ и компоненты программного обеспечения (VCL, LIB и др.).

- **Перезаписывающие вирусы** — вирусы данного типа записывают своё тело вместо кода программы, не изменяя названия исполняемого файла, вследствие чего исходная программа перестаёт запускаться. При запуске программы выполняется код вируса, а не сама программа.

- **Вирусы-компаньоны** — как и перезаписывающие вирусы, создают свою копию на месте заражаемой программы, но в отличие от перезаписывающих не уничтожают оригинальный файл, а переименовывают или перемещают его. При запуске программы вначале выполняется код вируса, а затем управление передаётся оригинальной программе.

  Возможно существование и других типов вирусов-компаньонов, использующих иные оригинальные идеи или особенности других операционных систем. Например, PATH-компаньоны, которые размещают свои копии в основном каталоге Windows, используя тот факт, что этот каталог является первым в списке PATH и файлы для запуска Windows в первую очередь будет искать именно в нём. Данным способом самозапуска пользуются также многие компьютерные черви и троянские программы.

- **Файловые черви** — создают собственные копии с привлекательными для пользователя названиями (например, Game.exe, install.exe и др.) в надежде на то, что пользователь их запустит.

- **Вирусы-звенья** — как и компаньон-вирусы, не изменяют код программы, а заставляют операционную систему выполнить собственный код, изменяя адрес местоположения на диске заражённой программы на собственный адрес. После выполнения кода вируса управление обычно передаётся вызываемой пользователем программе.

- **Паразитические вирусы** — это файловые вирусы, изменяющие содержимое файла, добавляя в него свой код. При этом заражённая программа сохраняет полную или частичную работоспособность. Код может внедряться в начало, середину или конец программы. Код вируса выполняется перед, после или вместе с программой, в зависимости от места внедрения вируса в программу.
- **Вирусы, поражающие исходный код программ** — вирусы данного типа поражают исходный код программы или её компоненты (OBJ-, LIB-, DCU-файлы), а также VCL- и ActiveX-компоненты. После компиляции программы оказываются встроенными в неё. В настоящее время широкого распространения не получили.

Каналы распространения

Дискеты — самый распространенный канал заражения в 80-90 гг. Сейчас практически не используется из-за появления более распространенных и эффективных каналов.

Флеш-накопители (флешки) — в настоящее время флеш-накопители повторяют судьбу дискет. Большое количество вирусов распространяется сегодня именно через съемные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, MP3-плееры, сотовые телефоны. Использование этого канала преимущественно обусловлено возможностью создания специального текстового файла Autorun.inf, в котором указывается программа, запускаемая Проводником Windows при открытии такого накопителя. Это основной источник заражения в настоящее время для компьютеров, не подключенных к сети Интернет.

Электронная почта — сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, т.е. в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на

специально созданную страницу, содержащую вирусный код. Некоторые вирусы, попав на компьютер, могут использовать адресную книгу пользователя для рассылки самого себя.

Системы обмена мгновенными сообщениями — также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и другим программам мгновенного обмена сообщениями.

Web-страницы — возможно также заражение через страницы Интернет, ввиду наличия на страницах Всемирной паутины различного активного содержимого: скриптов, ActiveX компонентов, Java-апплетов. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта (это опаснее всего, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи, зайдя на такой сайт, рискуют заразить свой компьютер.

Интернет и локальная сеть (черви). Черви – вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер. Уязвимости - это ошибки и недоработки в программном обеспечении, которые позволяют удаленно загрузить и выполнить машинный код, в результате чего вирус-червь попадает в операционную систему и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет. Хакеры и спамеры используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак.

4.2. Троянские программы

Название «троянская программа» происходит от названия «троянский конь» — деревянный конь, по легенде, подаренный древними греками жителям Трои, внутри которого прятались воины, впоследствии открывшие завоевателям ворота города. Такое название прежде всего отражает скрытность и потенциальную коварность истинных замыслов разработчика программы.

Троянская программа может в той или иной степени имитировать (или даже полноценно заменять) задачу или файл данных, под которые она маскируется (программу установки, прикладную программу, игру, прикладной документ, картинку). В том числе злоумышленник может собрать существующую программу с добавлением к её исходному коду троянских компонентов, а потом выдавать за оригинал или подменять его.

Схожие вредоносные и маскировочные функции также используются компьютерными вирусами, но в отличие от них троянские программы не умеют распространяться самостоятельно. Вместе с тем троянская программа может быть модулем вируса.

Распространение

Троянские программы помещаются злоумышленником на открытые ресурсы (файл-серверы, открытые для записи накопители самого компьютера), носители информации или присылаются с помощью служб обмена сообщениями (например, электронной почтой) из расчета на их запуск на конкретном, входящем в определенный круг или произвольном «целевом» компьютере.

Иногда использование троянов является лишь частью спланированной многоступенчатой атаки на определенные компьютеры, сети или ресурсы (в том числе третьи).

Типы тел троянских программ

Тела троянских программ почти всегда разработаны для различных вредоносных целей, но могут быть также безвредными. Они разбиваются на категории, основанные на том, как трояны внедряются в систему и наносят ей вред. Существует 6 главных типов:

1. Удалённый доступ.
2. Уничтожение данных.
3. Загрузчик.
4. Сервер.
5. Дезактиватор программ безопасности.

6. DDoS-атаки.

Цели

Целью троянской программы может быть:

- закачивание и скачивание файлов;
- копирование ложных ссылок, ведущих на поддельные вебсайты, чаты или другие сайты с регистрацией;
- создание помех работе пользователя (в шутку или для достижения других целей);
- похищение данных, представляющих ценность или тайну, в том числе информации для аутентификации, для несанкционированного доступа к ресурсам (в том числе третьих систем), выуживание деталей касательно банковских счетов, которые могут быть использованы в преступных целях, криптографической информации (для шифрования и цифровой подписи);
- шифрование файлов при кодовирусной атаке;
- распространение других вредоносных программ, таких как вирусы. Троян такого типа называется Dropper;
- вандализм: уничтожение данных (стирание или переписывание данных на диске, труднозамечаемые повреждения файлов) и оборудования, выведение из строя или отказ обслуживания компьютерных систем, сетей и т. п., в том числе в составе ботнета (организованной группы зомбированных компьютеров), например, для организации DoS-атаки на целевой компьютер (или сервер) одновременно со множества зараженных компьютеров или рассылки спама. Для этого иногда используются гибриды троянского коня и сетевого червя — программы, обладающие способностью к скоростному распространению по компьютерным сетям и захватывающие зараженные компьютеры в зомби-сеть;
- сбор адресов электронной почты и использование их для рассылки спама;

- прямое управление компьютером (разрешение удалённого доступа к компьютеру-жертве);
- шпионство за пользователем и тайное сообщение третьим лицам сведений, таких как, например, привычка посещения сайтов;
- регистрация нажатий клавиш (Keylogger) с целью кражи информации такого рода как пароли и номера кредитных карточек;
- получение несанкционированного (и/или дарового) доступа к ресурсам самого компьютера или третьим ресурсам, доступным через него;
- установка Backdoor;
- использование телефонного модема для совершения дорогостоящих звонков, что влечёт за собой значительные суммы в телефонных счетах;
- дезактивация или создание помех работе антивирусных программ и файрвола.

Симптомы заражения трояном

- Появление в реестре автозапуска новых приложений.
- Показ фальшивой закачки видеопрограмм, игр, порнороликов и порносайтов, которые вы не закачивали и не посещали.
- Создание снимков экрана.
- Открывание и закрывание консоли CD-ROM.
- Проигрывание звуков и/или изображений, демонстрация фотоснимков.
- Перезапуск компьютера во время старта инфицированной программы.
- Случайное и/или беспорядочное отключение компьютера.

Методы удаления

Поскольку трояны обладают множеством видов и форм, не существует единого метода их удаления. Наиболее простое решение заключается в очистке папки Temporary Internet Files или нахождении вредоносного файла и удалении его вручную (рекомендуется Безопасный Режим). В принципе, антивирусные программы не способны обнаруживать и удалять трояны. Однако при регулярном обновлении антивирусной базы антивирус способен заблокировать запуск и исполнение троянской программы. Если антивирус не способен отыскать троян, загрузка ОС с альтернативного источника может дать возможность антивирусной программе обнаружить троян и удалить его. Чрезвычайно важно для обеспечения большей точности обнаружения регулярное обновление антивирусной базы данных.

Маскировка

Многие трояны могут находиться на компьютере пользователя без его ведома. Иногда трояны прописываются в Реестре, что приводит к их автоматическому запуску при старте Windows. Также трояны могут комбинироваться с легитимными файлами. Когда пользователь открывает такой файл или запускает приложение, троян запускается также.

Принцип действия трояна

Трояны обычно состоят из двух частей: Клиент и Сервер. Сервер запускается на машине-жертве и следит за соединениями от Клиента, используемого атакующей стороной. Когда Сервер запущен, он отслеживает порт или несколько портов в поиске соединения от Клиента. Для того чтобы атакующая сторона подсоединилась к Серверу, она должна знать IP-адрес машины, на которой запущен Сервер. Некоторые трояны отправляют IP-адрес машины-жертвы атакующей стороне по электронной почте или иным способом.

Как только с Сервером произошло соединение, Клиент может отправлять на него команды, которые Сервер будет исполнять на машине-жертве. В настоящее время благодаря NAT-технологии по-

лучить доступ к большинству компьютеров через их внешний IP-адрес невозможно. И теперь многие трояны соединяются с компьютером атакующей стороны, который установлен на приём соединений, вместо того, чтобы атакующая сторона сама пыталась соединиться с жертвой. Многие современные трояны также могут беспрепятственно обходить файрволы на компьютере жертвы.

Трояны чрезвычайно просты в создании на многих языках программирования. Простой троян на Visual Basic или C++ с использованием Visual Studio может быть создан в не более чем 10 строчках кода.

4.3. Spyware

Что такое spyware?

Spyware — программа, которая скрытным образом устанавливается на компьютер с целью полного или частичного контроля над взаимодействием между пользователем и компьютером без согласия пользователя.

В то время как термин Spyware предполагает программу, тайным образом отслеживающую поведение пользователя, функции Spyware простираются далеко за пределы простого отслеживания.

Spyware могут заниматься сбором различных типов личной информации и используются для:

- отслеживания привычек пользования Интернетом и посещаемые сайты (Tracking Software);
- контроля нажатий клавиш на клавиатуре компьютера (Keyloggers);
- контроля скриншотов экрана монитора компьютера (Screen Scraper);
- несанкционированного удалённого контроля и управления компьютерами (Remote Control Software) — Backdoors, Botnets, Droneware;

- несанкционированного анализа состояния систем безопасности (Security Analysis Software) — Hacker Tools, Port and vulnerability scanners, Password crackers.

Spyware могут также вмешиваться в контроль пользователя над компьютером с других сторон, например:

- инсталлируя дополнительные программы;
- перенаправляя активность браузеров, что влечёт за собой посещение веб-сайтов вслепую с риском заражения вирусами.

Spyware могут даже менять установки в компьютере для несанкционированного внесения изменений в компьютерную систему (System Modifying Software) — например Hijackers, Rootkits, результатом чего являются снижение скорости соединения с Интернетом или потеря соединения как такового, открывание других домашних страниц или удаление тех или иных программ.

В настоящий момент существует множество определений и толкований термина Spyware. Поэтому в данной статье за основу приняты устоявшиеся определения этого термина, применяемые Anti-Spyware Coalition — коалицией, в которой состоят многие крупные производители антишпионского и антивирусного программного обеспечения. В соответствии с толкованием Anti-Spyware Coalition данный термин может иметь два значения:

- в узком смысле Spyware — это мониторинговый программный продукт, установленный и применяемый без должного оповещения пользователя, его согласия и контроля со стороны пользователя, то есть несанкционированно установленный. Именно в этом узком смысле термин Spyware (в переводе англ. Spy — шпион и Software — программное обеспечение) соответствует своему дословному переводу, то есть *шпионское программное обеспечение*;
- в более широком смысле термин Spyware используется как синоним того, что Anti-Spyware Coalition называет «Spyware плюс Другие Потенциально Нежелательные Технологии».

В отличие от вирусов и сетевых червей Spyware обычно не саморазмножается. Подобно многим современным вирусам, Spyware внедря-

ется в компьютер преимущественно с коммерческими целями. Типичные проявления включают в себя демонстрацию всплывающих рекламных окон, кражу персональной информации (включая финансовую, например номеров кредитных карт), отслеживание привычки посещения веб-сайтов или перенаправление адресного запроса в браузере на рекламные или порносайты.

Пути инфицирования

Spyware напрямую не распространяются по образу сетевых червей и вирусов; как правило, инфицированная система не пытается передать инфекцию другим компьютерам. Вместо этого Spyware попадает в систему посредством обмана пользователя или через уязвимости системы. Большинство Spyware инсталлируются без ведома пользователя.

Поскольку пользователи стремятся не инсталлировать программы, которые, как они знают, могут подорвать целостность системы и подвергнуть опасности личные данные, Spyware обманывают пользователей, комбинируясь в единое целое с популярными программами, например Kazaa, или же жульническим путём заставляют пользователя их инсталлировать (метод троянов). Некоторые фальшивые программы маскируются под программы безопасности, сами являясь Spyware.

Распространители Spyware обычно представляют свой продукт как что-то полезное, например веб-ускоритель или полезный программный агент. Пользователь скачивает и инсталлирует программу, сразу не подозревая, что это может принести вред.

Например, BonziBuddy, программа, упакованная со Spyware и предназначенная для целевой группы ДЕТИ, утверждает, что «он будет исследовать Интернет с тобой как твой самый закадычный друг. Он может говорить, ходить, шутить, бегать по страницам, искать, отправлять e-mail и скачивать (файлы), как никто другой из твоих друзей! У него даже есть способность сравнивать цены на товары, которые тебе понравились, и он будет помогать тебе экономить деньги. Он самый лучший, он бесплатный!».

4.4. Лечим от вирусов

Антивирусные программы

Обязательно необходимо установить на свой компьютер антивирусную программу (так называемый антивирус). Большая часть проблем в работе Windows возникает именно из-за внесенных на компьютер вирусов. Очень хорошими антивирусными программами являются российские Dr.Web и Антивирус Касперского. Более удобным для начинающих является Dr.Web, но зато Антивирус Касперского позволяет более гибко настраивать проверку на вирусы (это понравится опытным пользователям). Я же рекомендую использовать бесплатный антивирус Avast! (рис. 4.1). Он очень хорошо защищает от вирусов (не хуже платных программ), скачать его можно на сайте www.avast.com.

Обратите внимание, что, когда вы установите себе антивирусную программу, она всегда будет автоматически проверять основные системные файлы на наличие вирусов. Однако необходимо периодически вручную запускать проверку всех файлов на диске. Кроме того необходимо проверять на наличие вирусов все файлы, которые вы записываете в ком-

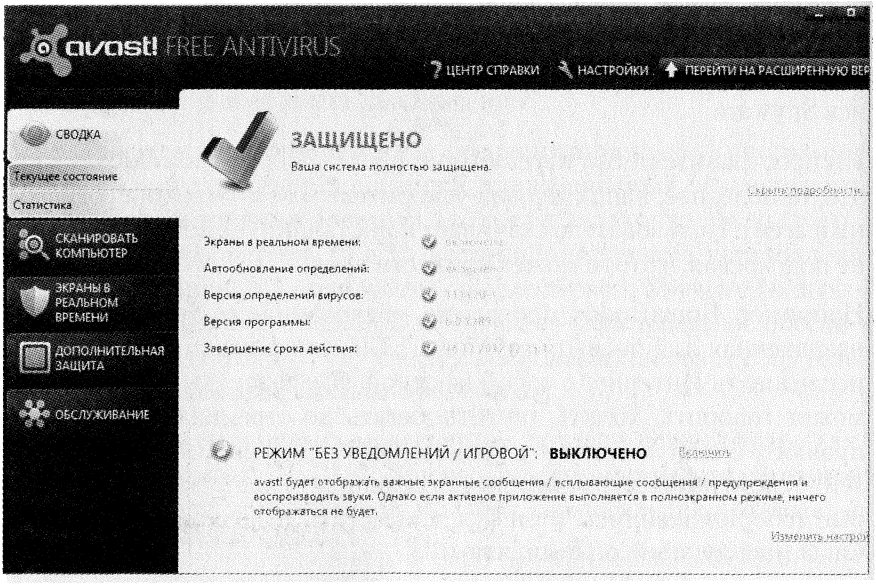


Рис. 4.1. Бесплатный антивирус Avast!

пьютер. Заведите себе за правило: переписываете, например, с флешки какой-либо файл – сначала проверьте его на вирусы.

И еще, не забывайте со временем обновлять антивирусные базы для своего антивируса. Ведь с каждым днем появляются все новые и новые вирусы.

Проверка файлов на вирус

После установки антивирусной программы (например, Антивируса Касперского) в контекстном меню, вызываемом щелчком правой кнопки мыши по значку файла, появляется специальная команда **Проверить на вирусы** (см. рис. 4.2).

Сама процедура проверки каких-либо файлов антивирусом при этом выглядит следующим образом:

1. Выделите файлы, которые вы хотите проверить на наличие вирусов.

2. Щелкните по выделенным файлам правой кнопкой мыши и в контекст-ном меню выберите **Проверить на вирусы**.

После этого они будут проверены на вирусы. Если таковые будут найдены, то вам будет предложено либо вылечить такие файлы, либо вообще их удалить (иногда лечение невозможно). Обратите внимание, что антивирус может также просто предупреждать о различных подозрительных действиях, многие из которых могут быть вполне миролюбивыми.

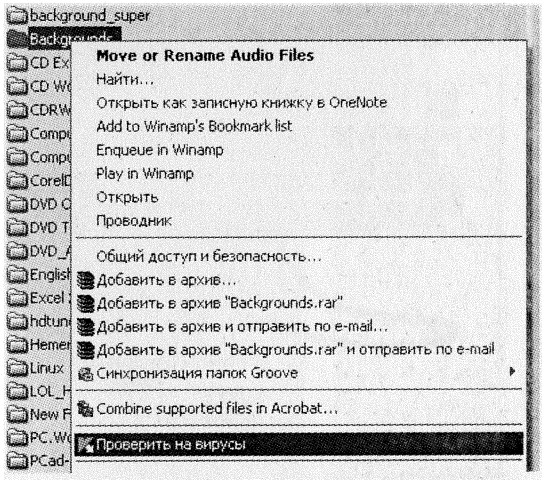
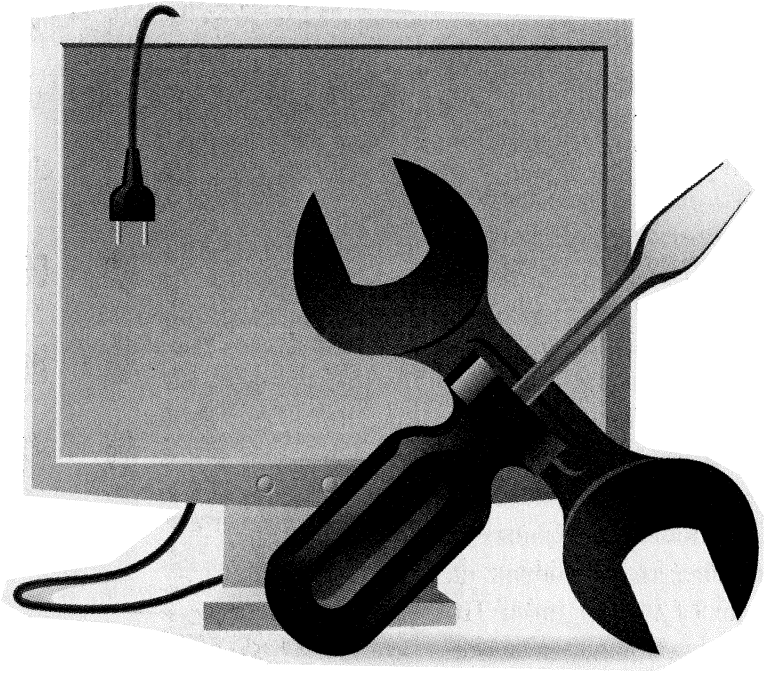


Рис. 4.2. Команда проверки на вирусы в контекстном меню

ГЛАВА 5.

ПОТЕРЯЛИСЬ ФАЙЛЫ, ДОКУМЕНТЫ, ФОТОГРАФИИ НА КОМПЬЮТЕРЕ. КАК НАЙТИ?



5.1. Поиск файлов в Windows XP

В Windows XP приступить к поиску можно несколькими способами в зависимости от того, что вы сейчас делаете и что у вас открыто на Рабочем столе:

- Если у вас открыто какое-либо окно папки, то можете прямо в нем нажать на кнопку **Поиск,** и в левой части окна появится одноименная панель, с помощью которой и будет происходить поиск.

- Если же у вас никакого окна папки не открыто, то приступить к поиску можно, выбрав **Пуск → Поиск**. Тогда на экране появится окно **Результаты поиска** (пока еще пустое) с открытой слева панелью **Поиск**.

Далее в расположенной слева панели щелкните мышкой по ссылке **Файлы и папки**. В результате на панели появится несколько полей, в которых вы сможете указать параметры поиска (рис. 5.1). Так, в поле **Поиск в** можно выбрать диск, папку или сетевой ресурс, в котором требуется производить поиск. Если вы открывали панель

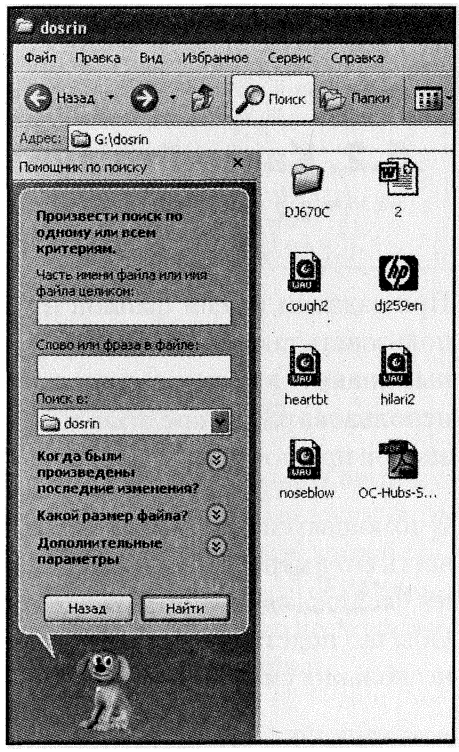


Рис. 5.1. Поиск в Windows XP

Поиск из какого-либо окна папки, то по умолчанию вам будет предложено производить поиск именно в этой папке.

В поле **Часть имени файла или имя целиком** понятно, что нужно вводить. При вводе в это поле сначала открывается список с введенными ранее значениями. Поэтому, если вы ранее уже производили поиск данного конкретного файла, то вы сможете просто выбрать его в списке. В поле **Слово или фраза в файле** вы можете указать текстовый фрагмент, который должен присутствовать в найденных файлах.

Начать поиск можно, нажав на кнопку **Найти**. Через некоторое время в правой части окна отобразится список найденных файлов и папок. В ходе поиска слева будет отображаться, где именно в данный момент идет поиск.

5.2. Как найти нужный файл, если вы помните только часть его имени?

При задании имени файлов и папок для поиска вы можете использовать так называемые подстановочные знаки. **Подстановочные знаки – это вводимые с клавиатуры знаки, которые можно использовать для представления одного или нескольких других знаков при поиске.**

С помощью них вы, во-первых, сможете отыскать файл, зная лишь часть его имени, а во-вторых, вы сможете отыскивать целые группы файлов (папок), содержащие в названия определенные буквы. Обычно подстановочные знаки используются вместо одного или нескольких символов (букв, цифр).

Описание подстановочных знаков Windows приведено в табл. 5.1.

Таблица 5.1. *Подстановочные знаки*

Подстановочный знак	Использование
Звездочка (*)	Звездочка может использоваться для задания произвольной группы символов, включая пустой. Например, если в качестве предмета поиска укажете *rut**, то найдены будут все файлы и папки, начинающиеся на буквосочетание *rut* (например, *rutan.exe*, *ruty.com*, *rutenol.doc*). При этом не имеет никакого значения, сколько символов стоит после буквосочетания *rut*. Можно также найти все файлы, закачивающиеся на *rut*. Тогда вы должны указать в качестве запроса **rut*. И, например, можно найти все файлы, просто содержащие в своем названии буквосочетание *rut*. Для этого достаточно ввести **rut**.
Вопросительный знак (?)	Вопросительный знак может использоваться для замены одного знака в имени. При этом можно использовать несколько вопросительных знаков подряд. Например, если надо найти все файлы, начинающиеся на *rut*, но содержащие только 6 символов в названии, в качестве запроса на поиск вы должный указать *rut???*. При этом не будут найдены слова на из четырех, пяти, семи и т.д. букв, а только из шести. Например, не будут найдены файлы *rutan.exe* и *rutenol.doc*, а файл *rutera.doc* будет найден.

5.3. Поиск в Windows 7 и 8

Удобство поиска в Windows 7 и 8 на голову превосходит систему поиска своих предшественниц. Те, кто пересел на «семерку» или «восьмерку» сразу же с XP, сильно удивятся прорыву в данной области функционирования операционной системы. Ведь если раньше поиск того же файла занимал от десятков секунд, до нескольких минут, то сейчас весь процесс стал занимать доли секунды.

Дело в том, что в Windows 7/8 в основу поиска взят принцип индексирования, что коренным образом меняет его алгоритм. Ин-

дексированием называется процесс собирания, разбора и сохранения данных с целью облегчить быстрый и точный поиск информации. Windows использует индекс для быстрого поиска на компьютере наиболее распространенных типов файлов. Индексом становятся такие свойства файлов, как автор документа, дата создания, тип, путь к папке, теги в MP3 файлах, различные ключевые слова и многое другое. Как только вы создали, изменили или удалили файл – тут же происходит его индексирование. Тоже самое происходит и для папок. Поэтому данные поиска в любой момент являются актуальными.

Простой поиск

Для того, чтобы осуществить простейший поиск, щелкните кнопку **Пуск** и введите в поле ввода искомый объект (рис. 5.2).

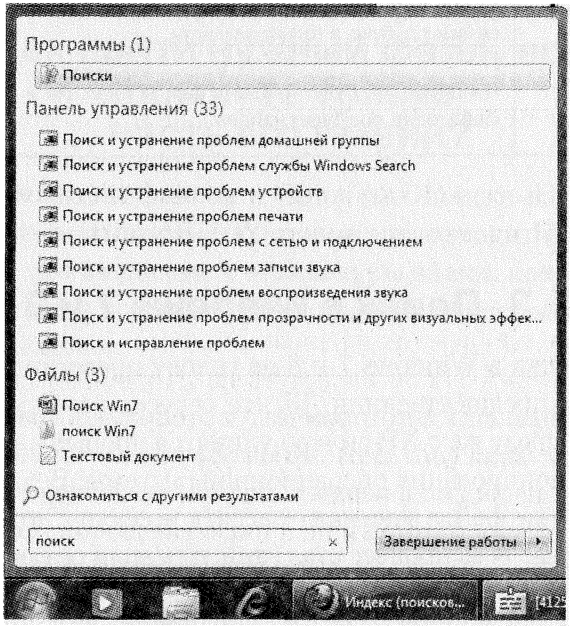


Рис. 5.2. Простейший поиск

Обратите внимание, что все результаты поиска, моментально сформированные, группируются по разделам: **Программы**, элементы **Панели управления** и **Файлы**. Разделов может быть еще больше. Их количество зависит только от вашего запроса. Стоит признать удобность данного решения, так как пользователю теперь не придется ломать голову, к какому типу относятся найденные объекты.

Вернемся в рисунку 1 и заметим, что кроме найденных файлов поисковая система нашла нам программу и элементы Панели управления. Это означает то, что теперь вам не нужно будет запускать нужную программу после прохождения утомительного пути по многоуровневому меню Пуск. Теперь вам достаточно лишь ввести начальные символы названия нужного приложения и вы тут же получите его в списке результатов поиска. Если программ, имеющих одинаковое начало в названии несколько, то вам останется лишь выбрать нужную. Теперь вас не испугает никакой огромный список установленных приложений.

Если вы имеете портабельные приложения и хотите, чтобы они тоже попадали в результаты поиска, то нужно добавить их ярлыки в папку **C:\Users\YOURNAME\AppData\Microsoft\Windows\Start Menu\Programs,** где вместо **YOURNAME** введите свое имя пользователя.

Щелкнув на любой из найденных объектов, вы тут же откроете или запустите его. Если щелкнуть на найденный раздел, то откроется окно поиска, в котором будут отображены результаты поиска этого раздела (рис. 5.3). Кроме меню Пуск, вы можете ввести поисковый запрос в верхнем правом поле ввода любого окна Windows. Однако, где бы вы не производили поиск, его результаты в большей мере зависят от того, как настроено индексирование файлов.

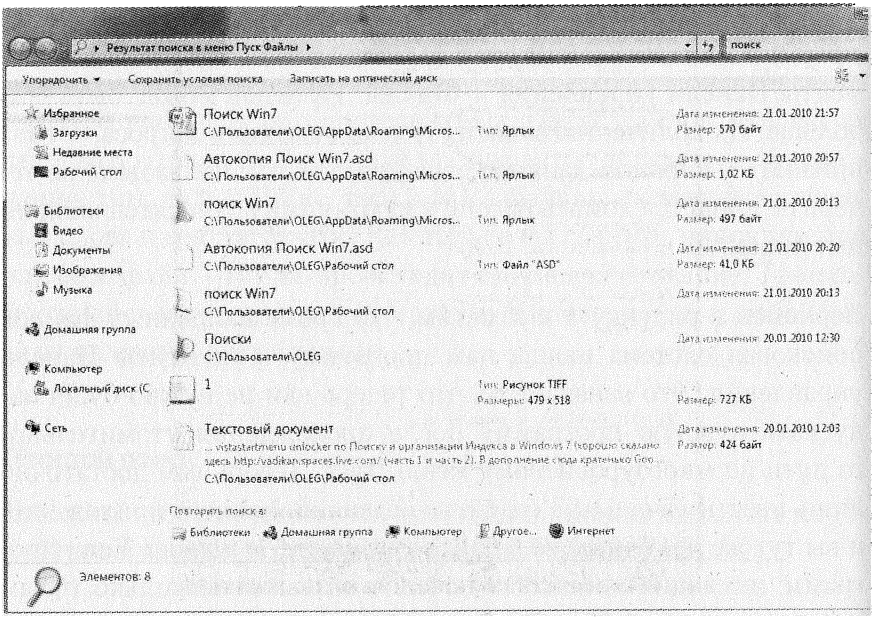


Рис. 5.3. Результаты поиска раздела «Файлы»

Индексирование

Если поиск выполняется в неиндексированных расположениях, он может занять продолжительное время, так как во время поиска Windows должна проверить каждый файл, находящийся в этих расположениях. Для повышения скорости поиска в дальнейшем можно добавить эти расположения в индекс. Чтобы сделать это, а также многое другое для повышения продуктивности поиска, щелкните кнопку Пуск и введите в поисковой строке **Параметры индексирования**. Посмотрите на список результатов поиска. Нас здесь будет интересовать два рядом расположенных элементов Панели управления **Параметры индексирования** и **Параметры папок** (рис. 5.4).

Сначала щелкните строку **Параметры папок**. Откроется одноименное окно. Перейдите во вкладку **Поиск** (рис. 5.5).

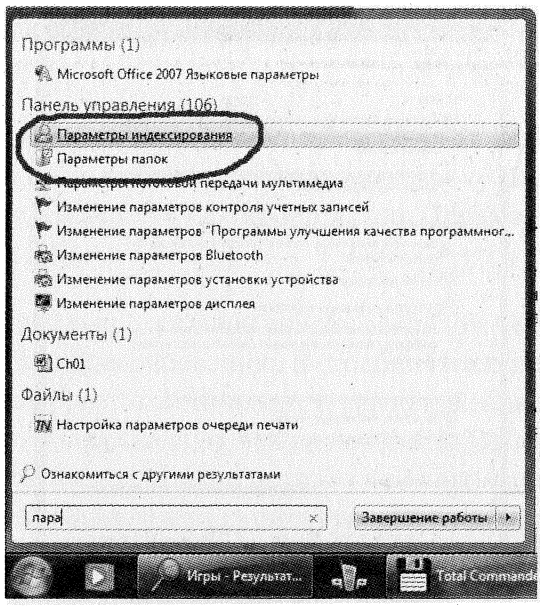


Рис. 5.4. Результаты поиска

Открыть окно можно и другими способами, например, открыть любую папку, щелкнуть **Упорядочить** и в появившемся меню выбрать пункт **Параметры папок и поиска**. В любом случае результат будет одинаковым.

В окне **Параметры папок** вы можете установить собственные правила поиска файлов в папках. По умолчанию поиск по имени файлов и его содержимому ведется только в проиндексированных расположениях. В неиндексированных расположениях поиск ведется лишь по имени. Но вы можете сделать и здесь поиск по содержимому.

Однако это сильно увеличит время поиска. Если вы желаете, чтобы поиск осуществлялся только при полном совпадении введенного запроса, то снимите флажок **Поиск частичных совпадений**. Если установить флажок **Использовать языковый поиск**, то при вводе поискового запроса Windows 7/8 будет пытаться использо-

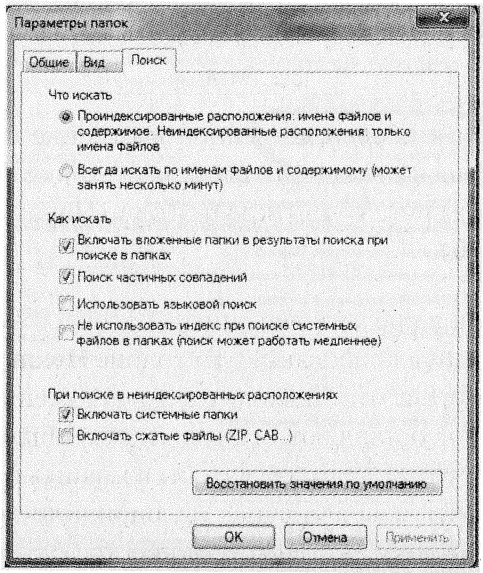


Рис. 5.5. Параметры папок

вать морфологические особенности языка. Однако, судя по проведенным тестам, с русским языком у Windows 7/8 пока есть проблемы. Например, не получается найти файл с названием «Дубовый.txt», если вводить запрос «дубовая». Поэтому языковой поиск пока можно отключать в целях экономии системных ресурсов.

Также не стоит включать опцию **Не использовать индекс при поиске системных файлов в папках, так как это тоже очень сильно замедлит процесс поиска**. Однако, при выключенном индексировании системных файлов, параметр лучше включить. Снимите флажок **Включать системные файлы**, чтобы не проводить поиск системных файлов.

Очень многие пользователи в целях экономии места помещают множество документов в архивы. По умолчанию содержимое архивов не подлежит поиску. Но если включить параметр **Включать сжатые файлы**, то поиск будет проводиться и по содержи-

мому тех архивов, которые Windows 7/8 способна открыть своими средствами.

Теперь перейдем к непосредственной настройке параметров индексирования поиска. Для этого щелкните строку **Параметры индексирования** (см.рис. 5.4). Откроется окно **Параметры индексирования** (рис. 5.6).

Вашему вниманию представлен список расположений (мест), которые подлежат индексированию. В столбце **Исключить** перечислены папки, которые хотя и входят в расположение индексируемых объектов, но составляют исключение из общего правила, то есть не индексируются. Для того, чтобы изменить индексируемые объекты, путем исключения существующих или добавления новых, щелкните кнопку **Изменить**. Откроется окно **Индексируемые расположения** (рис. 5.7).

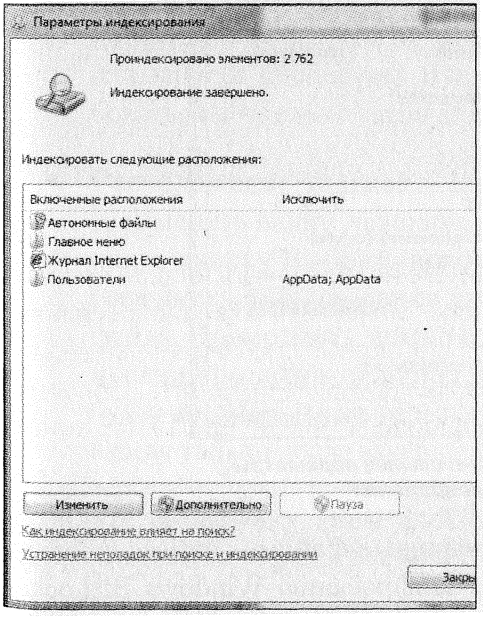


Рис. 5.6. Параметры индексирования

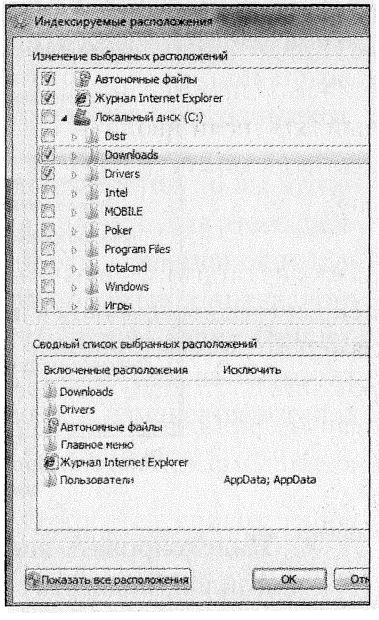


Рис. 5.7. Изменение индексируемых расположений

Окно состоит из двух вертикально расположенных областей. В верхнем отображена в древовидном виде структура содержимого жесткого диска. Флажками отмечены индексируемые участки. Щелкая на узлы, вы можете раскрывать ветви дерева диска. Отметьте флажками нужные папки. Они тут же будут отображаться в нижней области. Как только вы выберите все нужные места, щелкните кнопку **ОК**.

Теперь щелкните кнопку **Дополнительно**. Откроется окно **Дополнительно**, состоящее из двух вкладок. Вкладка **Параметры индексирования** состоит из следующих опций (Рис. 5.8):

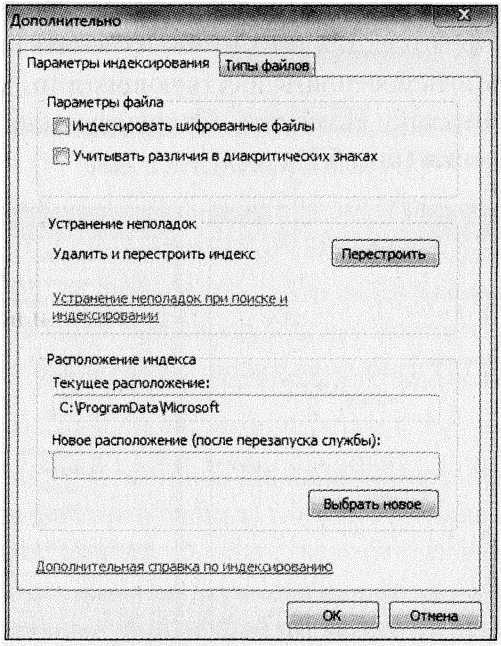


Рис. 5.8. Дополнительные параметры индексирования

- **Индексировать шифрованные файлы** – индексирование файлов, подвергнутых шифрованию Windows BitLocker или другими программами шифрования. При каждом из-

менении этого параметра будет проводиться процедура перестройки индекса.

- **Учитывать различия в диакритических знаках** — если в имени файлов или папок часто используются диакритические знаки (небольшие знаки, добавляемые к букве для изменения произношения слов), можно настроить индекс, чтобы слова с диакритическими знаками распознавались по отдельности. По умолчанию Windows распознает диакритические знаки в соответствии с используемым языком системы. Если установить флажок, то все диакритические знаки будут распознаваться.

- **Удалить и перестроить индекс** – если вы заметите, что файл, который находится в индексированном расположении, не появляется в результатах поиска, значит пришло время провести процедуру обслуживания индекса, а попросту – перестроить. Щелкните кнопку **Перестроить** для запуска процедуры. Будьте готовы, что может потребоваться несколько часов для перестройки всего индекса.

- **Расположение индекса** – если потребуется, то вы можете изменить папку расположения индекса. Для этого щелкните кнопку **Выбрать новое** и в открывшемся окне дерева диска выбрать папку для расположения индексного файла. Прямо здесь можно создать новую папку. При изменении расположения индекса служба поиска Windows будет автоматически перезапущена, и изменения вступят в силу только после завершения перезапуска.

Перейдите во вкладку **Типы файлов**. Откроется список типов файлов с описанием фильтров (рис. 5.9).

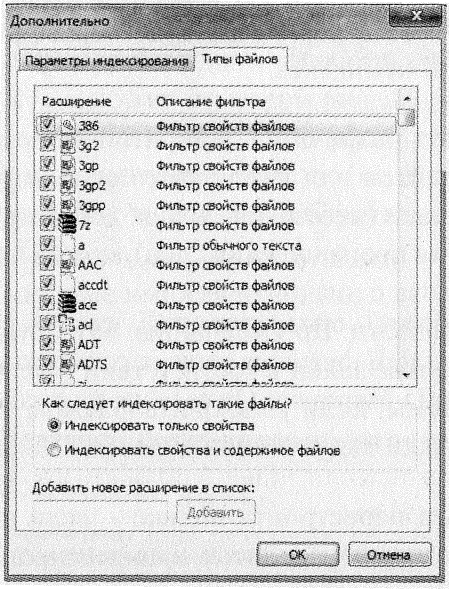


Рис. 5.9. Настройка индексирования типов файлов

Если выделить любой тип файлов, внизу окна можно увидеть, что именно будет индексироваться у файлов с данным расширением: только свойство либо свойство и содержимое файла. Вы можете поменять данный параметр у любого типа файлов либо вообще исключить любой тип из списка индексирования. Если же нужного типа файла нет в списке, то введите его в поле **Добавить новое расширение в список** (например, «DFT») и щелкните кнопку **Добавить**. Выберите **Индексировать только свойства** или **Индексировать свойства и содержимое файлов** и затем нажмите кнопку **ОК.**

Альтернативные виды поиска

Для осуществления поиска в Windows имеется специальное поисковое окно. Для его открытия нажмите комбинацию клавиш **Win+F** (рис. 5.10).

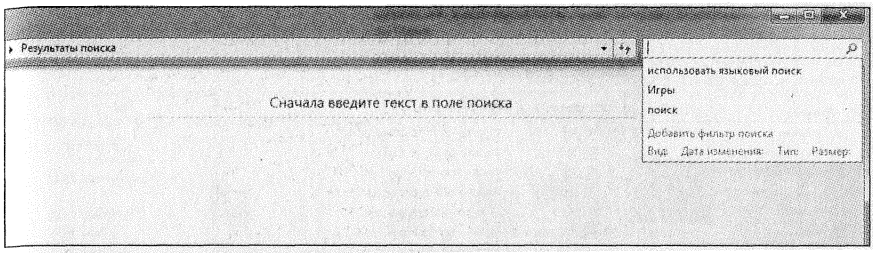


Рис. 5.10. Окно поиска Windows

Если сказать честно, то мы не понимаем смысла в наличии данного окна, так как здесь нет ничего сверх того, что можно сделать в любом другом окне Windows. Окно содержит такое же поисковое поле ввода, имеет те же самые фильтры поиска. Уникальность состоит в том, что в окне нет ничего лишнего, кроме поискового запроса и его результатов.

Расширенный поиск

Если поиск с помощью простых методов не увенчался успехом, то вы можете расширить область поиска, добавив различных расположений. Например, вы ищете рисунок в библиотеке **Изображения**. Однако он запросто может оказаться в любом другом месте. Например, осуществив поиск, вы получаете неудовлетворительный результат (рис. 5.11).

Внизу списка результатов поиска в разделе **Повторить поиск** вы можете расширить область поиска с помощью следующих кнопок:

- **Библиотеки** – расширение поиска до уровня всех библиотек
- **Компьютер** – поиск по всему компьютеру, который будет заметно медленнее, так как будут задействованы неиндексируемые расположения.

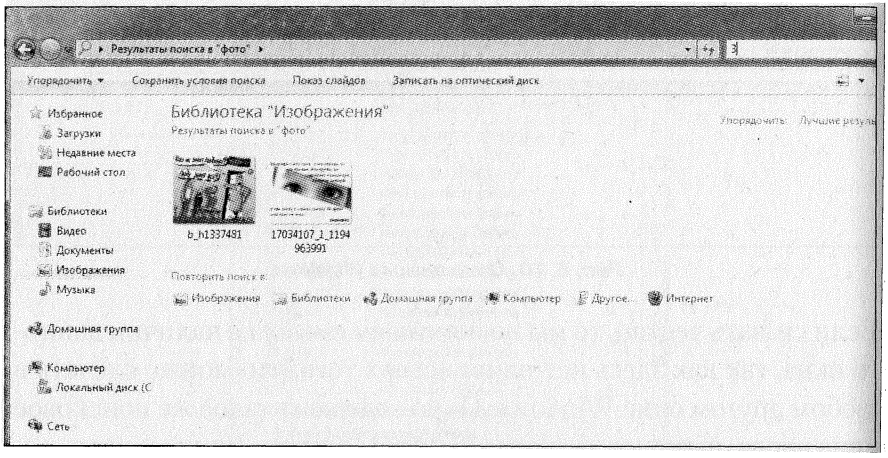


Рис. 5.11. Поиск рисунка в библиотеке «Изображения»

- **Другое** – выполнение поиска в конкретных расположениях, которые нужно будет выбрать самостоятельно. Если вы примерно догадываетесь о папке расположения файла, то выберите её, что заметно ускорит поиск.

- **Интернет** – поиск в Интернете в веб-браузере и его службе поиска, выбранной по умолчанию.

- **Домашняя или Рабочая группы** – поиск будет вестись в сети на уровне выбранной группы.

В зависимости от библиотеки, в которой вы будете осуществлять поиск, вам будут доступны различные фильтры. Пользуясь ими, вы сможете заметно повысить результаты поиска. Например, в библиотеке **Изображения** доступны следующие фильтры: **Дата съемки**, **Ключевые слова**, **Тип и другие** (рис. 5.12).

В библиотеке Видео доступны фильтры поиска **Продолжительность** и **Дата создания, Тип, Дата изменения и другие** (рис. 5.13).

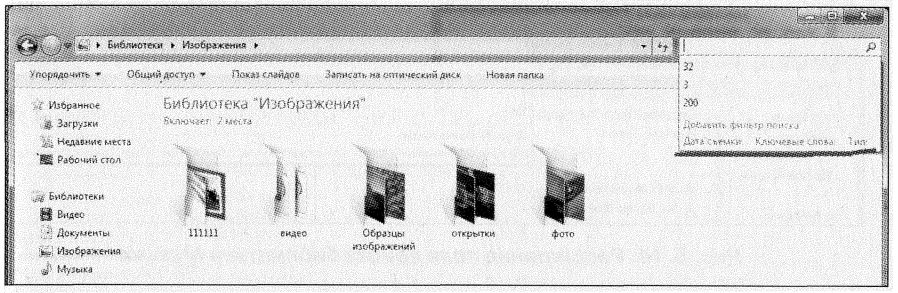


Рис. 5.12. Фильтры поиска библиотеки «Изображения»

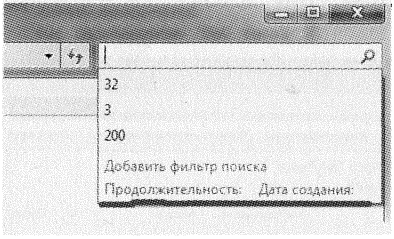


Рис. 5.13. Фильтры поиска библиотеки «Видео»

В библиотеке Документы доступны фильтры **Авторы**, **Тип**, **Дата изменения и другие**. В библиотеке Музыка можно воспользоваться фильтрами **Альбом**, **Исполнители**, **Жанр и другие**.

Причем количество отображаемых фильтров в поле поиска зависит от ширины этого поля. Расширьте поле ввода путем перетаскивания левой границы и вы увидите дополнительные фильтры (рис. 5.14).

Обратите внимание, что к вышеперечисленным фильтрам библиотеки Музыка прибавились **Продолжительность**, **Путь к папке**, **Год**, **Оценка** и **Название**.

Итак, мы рассмотрели, какие бывают фильтры в зависимости от типа выбранной библиотеки. Осталось разобрать, как ими пользоваться. Оказывается, что это очень просто. Просто щелкните

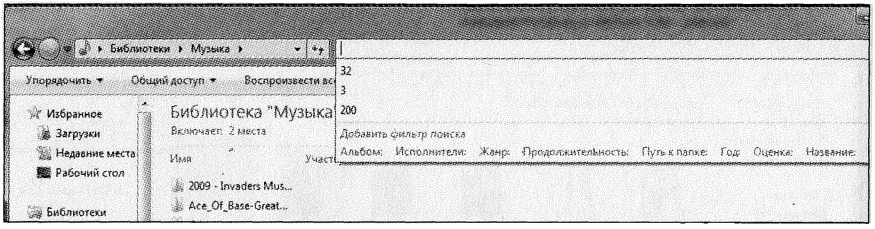


Рис. 5.14. Расширение поля поиска библиотеки Музыка

нужный фильтр в поисковом поле и выберите нужное его значение. Например, выберем в качестве фильтра поиска в библиотеке Музыка жанр **House** (рис. 5.15).

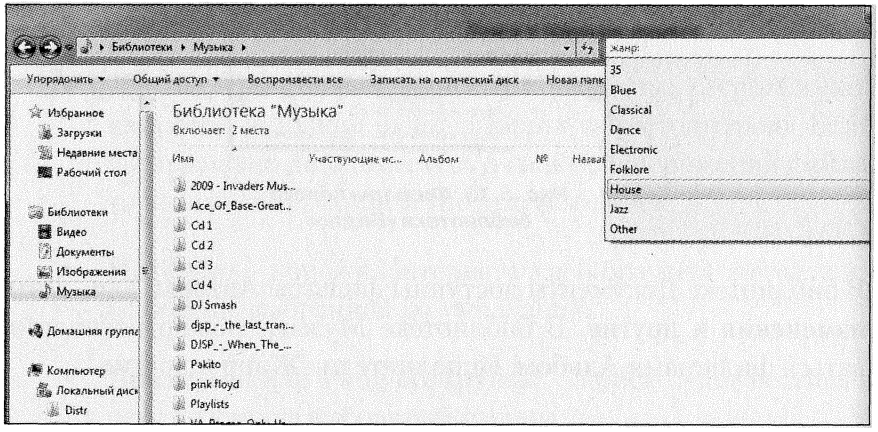


Рис. 5.15. Выбор жанра композиций

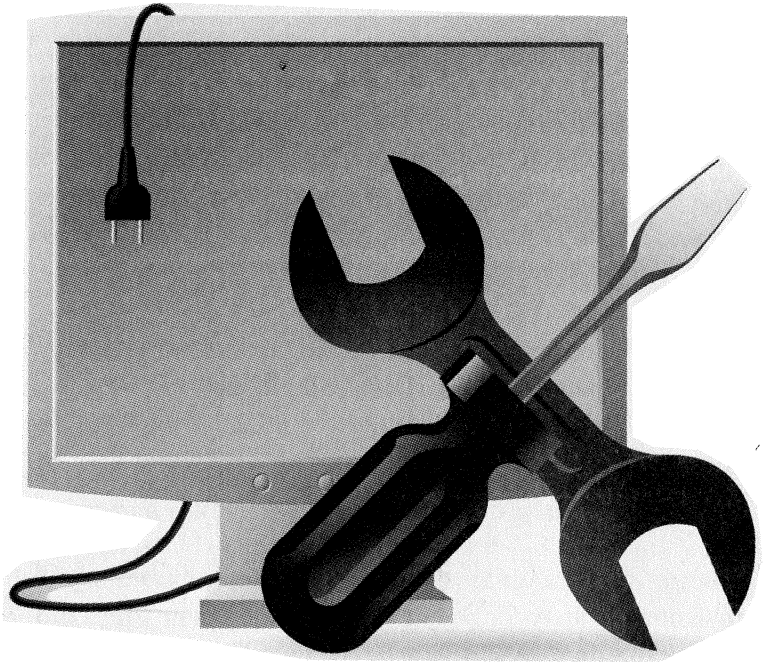
В результате из всей нашей аудиотеки компьютер отберет нам композиции с выбранным жанром (рис. 5.16).

Теперь нам остается выбрать либо исполнителя, либо нужный альбом. Хотя некоторым могут понадобиться, например, только длинные треки, либо только старые. Все в ваших руках, и с помощью системы фильтров вы легко доберетесь до нужного результата.

Рис. 5.16. Список композиций жанра House

ГЛАВА 6.

КОМПЬЮТЕР СТАЛ «ТОРМОЗИТЬ»



6.1. Зачистка системы от мусора и ошибок

Наверняка каждому владельцу или просто пользователю компьютера приходилось сталкиваться со следующей тенденцией. После приобретения нового ПК и установки необходимого программного обеспечения вы долгое время не нарадуетесь производительности вашего «электронного помощника или даже друга». Все просто «летает», обработка любой информации выполняется за считанные секунды. Однако проходит какое-то время (зависит от степени интенсивности использования и количества загружаемых приложений), и вы начинаете наблюдать, что происходит что-то не то. Ваш когда-то «строптивый жеребец» стал каким-то вяловатым. Периодически происходят небольшие торможения, длительность вычисления одной и той же операции заметно увеличилась.

Что же произошло? Ведь компьютер-то остался прежним, да и вроде вы не устанавливали более продвинутых программ, требующих повышенных запросов к аппаратной части вашего ПК. Некоторые могут подумать, что ваш компьютер «износился» или попросту «устал».

На самом деле все проще. В процессе установки программы в разные специализированные папки вашего жесткого диска устанавливается огромное количество вспомогательных файлов, в системный реестр в различные его ветви записывается великое множество информации. Но ведь мы удаляем программы после её ненадобности — скажете вы. Да, конечно, в процессе удаления

приложений с помощью специальной программы Uninstall (деинсталлятор) уничтожению подлежит большинство файлов, что приводит к значительному освобождению дискового пространства. Однако множество вспомогательных файлов и записей реестра остаются нетронутыми. Ведь в процессе работы с тем или иным приложением, в особенности играя в игры, создается множество всяких файликов, которые содержат специфическую информацию о совершенных вами действиях, например сохранение результатов пройденного пути в игре-квесте или создание резервной копии документа и т.п. А ведь результаты работы деинсталлятора лежат на совести разработчиков программного продукта, и поэтому не каждый uninstall «добросовестно» выполнит свое дело и не оставит следов пребывания программы на вашем жестком диске. Хотя порой это бывает просто невозможно выполнить технически.

Вообще-то для того, чтобы полностью удалить программу со всеми её «хвостами», существуют специальные программы, которые устанавливаются сразу же после установки операционной системы и затем отслеживают жизнь всех приложений и «запоминают», где они «намусорили». И затем, при удалении какой-либо программы, эта утилита видит, где находятся её "хвосты", и соответственно подчищает их.

Но если ваш компьютер эксплуатируется уже значительное время, следовательно, «поздно пить Боржоми» и такой способ нам не подойдет. Поэтому сегодня выпущено множество утилит немного другого рода, которые помогают очистить ваш жесткий диск от мусора, оставшегося от бывших программ, а также совершить множество других полезных операций по «освобождению» вашего ПК от различного рода ненужной, даже вредной информации и файлов.

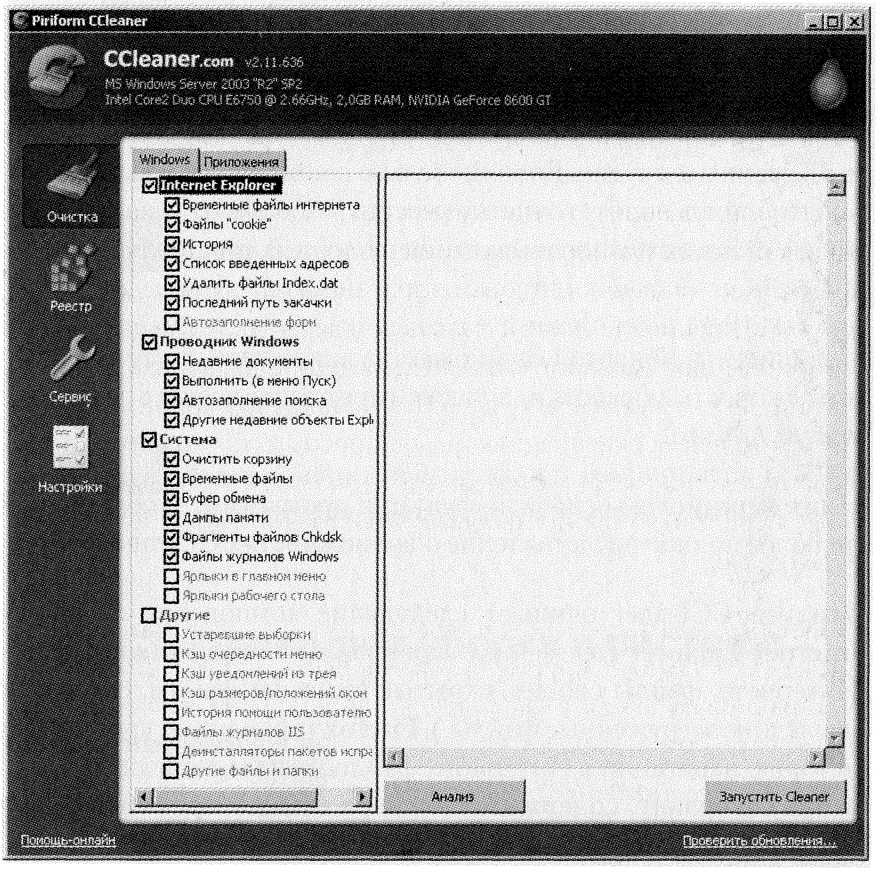


Рис. 6.1. Главное окно CCleaner

Одной из таких полезняшек является CCleaner, являющаяся детищем лондонской компании **Piriform**.

6.2. Возможности CCleaner

CCleaner является совершенно бесплатной программой для оптимизации вашей системы.

В первую очередь программа служит для очистки вашего жесткого диска от всякого рода «мусора». «Мусором» являются временные и неиспользуемые файлы, такие как история посещения вами страниц Интернета, cookies, фразы поисковых страниц, файлы Корзины и другие. Дополнительно с помощью CCleaner можно выполнить полную очистку реестра Windows от различных записей, оставшихся после удаления ненужных приложений и программ.

Отличительной чертой от множества аналогичных утилит является скорость обработки, а также отсутствие всякого рода Spyware и Adware.

Ниже перечислим основные функции программы, чтобы вы имели более полное представление о возможностях CCleaner.

Утилита CCleaner очищает следующие компоненты Windows: **Internet Explorer (**временные кэш-файлы, историю навигации в Интернете, файлы cookies, скрытые Index.dat файлы, ссылки на последние загруженные файлы.), **Firefox (**временные кэш-файлы, историю навигации в Интернете, файлы cookies, менеджер скачивания), **Корзину**, **содержимое буфера обмена**, **временные файлы Windows**, **лог-файлы**, **последние использованные документы, отображающиеся в меню Пуск**, **историю выполненных команд в меню Пуск.**

- 

Данный значок выбран по умолчанию. Выбрав его, вы сможете оптимизировать вашу систему, удалив неиспользуемые и временные файлы. Здесь же вы можете защитить свои личные тайны или секретную информацию, удалив все ссылки страниц, которые вы посещали ранее в Интернете, и ссылки на файлы, которые открывали.

-  Данный пункт программы имеет многие дополнительные опции, с помощью которых производится анализ реестра операционной системы и при выявлении различных проблем и несовместимостей выполняется их исправление.
-  Эта часть утилиты позволяет управлять установленными программами и приложениями (удалять, деинсталлировать, переименовывать), а также теми программами, которые запускаются автоматически при запуске операционной системы.
-  Данный пункт предоставляет вам широкие возможности по настройке различных обработок утилиты.

6.3. Проводим уборку в системе

Очистка жесткого диска

Щелкните значок  . В диалоговом окне отобразится список различных элементов Windows, которые утилита может очистить (см. рис. 6.1). Слева от каждого элемента расположен флажок. Вам нужно установить флажки тем элементам, которые вы желаете удалить, или же убрать у тех, которые хотите оставить.

То же самое нужно проделать с элементами сторонних приложений. Для этого щелкните вкладку **Приложения**. В диалоговом окне отобразится список приложений, поддерживаемых утилитой (рис. 6.2).

Установите/снимите флажки нужных элементов выбранных приложений.

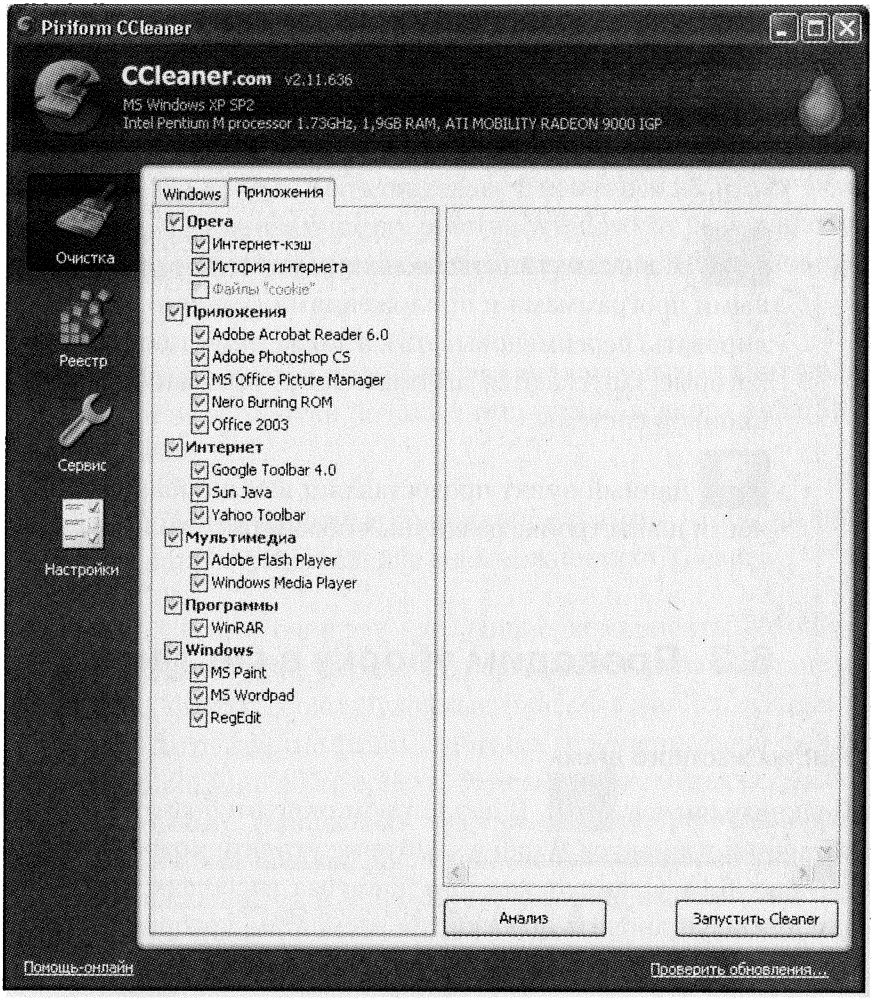


Рис. 6.2. Выбор элементов сторонних приложений для очистки

Далее вам предоставляется на выбор два варианта развития событий. Вы можете сразу же начать процесс удаления, для этого щелкните кнопку **Запустить Cleaner**. Но можно и подстраховаться и посмотреть, какие именно записи у выбранных элементов будут удалены. Для этого программа предлагает сделать анализ очищаемых элементов и показать вам, что будет удалено. Если вы выбираете второй вариант, щелкните кнопку **Анализ**.

В нашем примере сделаем анализ. Для этого щелкните кнопку **Анализ**. CCleaner начнет анализ удаляемых объектов и в итоге выдаст результат (рис. 6.3).

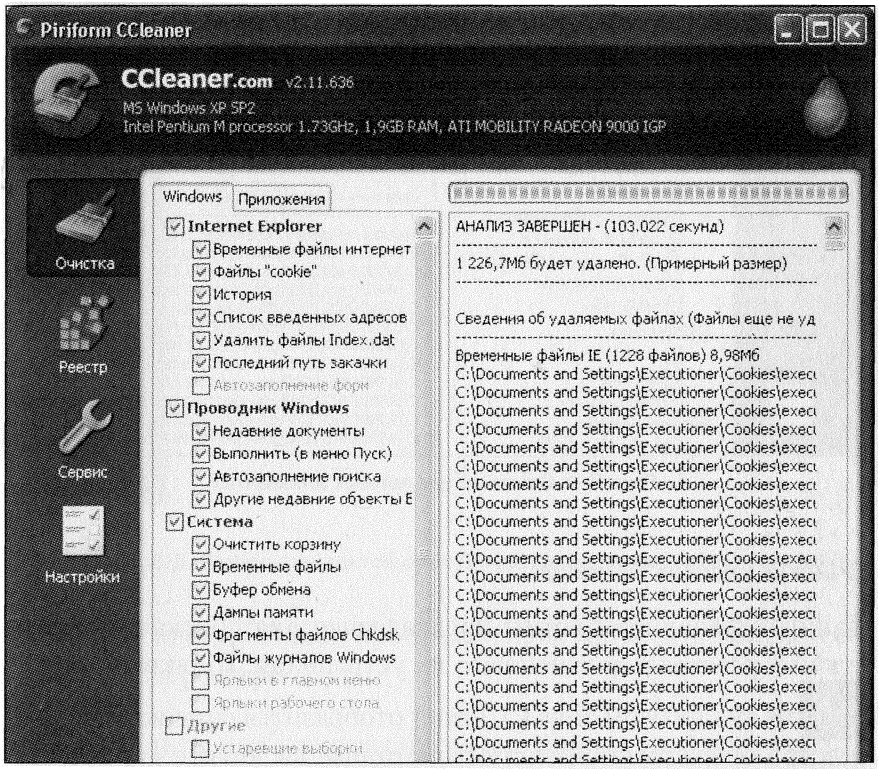


Рис. 6.3. Отчет об удаляемых файлах

Внимательно просмотрите этот список. Если вы заметите, что какие-то файлы вам понадобятся, снимите соответствующие флажки.

Как только вы откорректируете список очистки, можно приступить к физическому его уничтожению. Для этого щелкните кнопку **Запустить Cleaner.** Начнется очистка жесткого диска от выбранных файлов, и в окне утилиты отобразится список удаленных элементов (см. рис. 6.4).

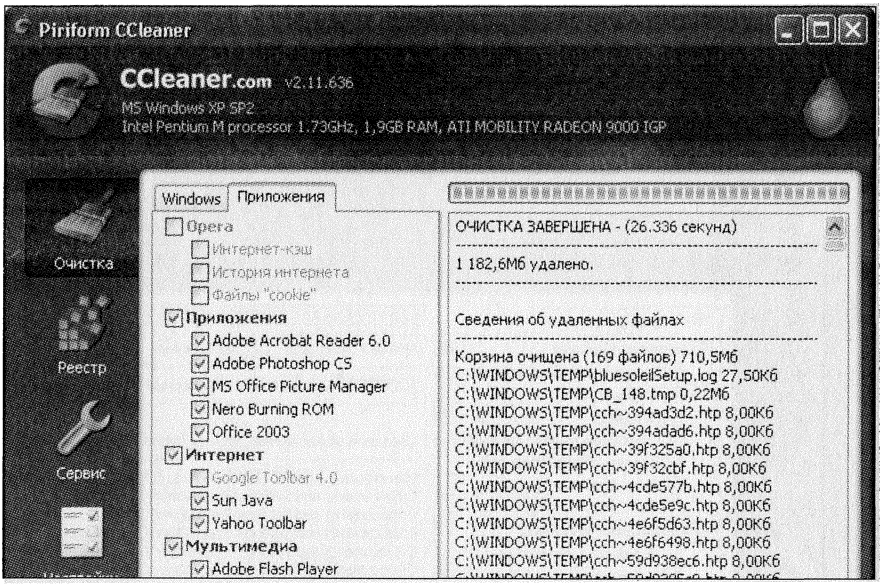


Рис. 6.4. Отчет об удаленных элементах

Очистка реестра Windows

Данный раздел программы предназначен для поиска несоответствий в реестре и дальнейшего их устранения. Щелкните значок  . В диалоговом окне CCleaner отобразится список элементов реестра операционной системы, которые вы хотите «привести в порядок».

С помощью флажков выберите нужные пункты.

Если вы думаете, что своими действиями можете «загубить» систему, то не бойтесь. CCleaner имеет в своем наличии комплект опций резервного копирования, поэтому, даже если вы когда-нибудь удалите что-то, что в дальнейшем вам потребуется, вы всегда сможете восстановить утраченные элементы.

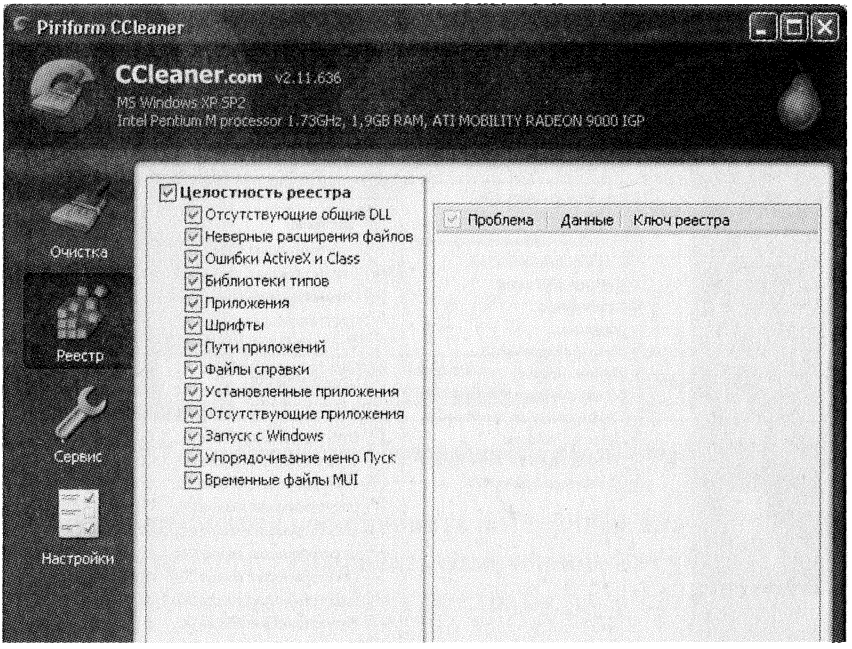


Рис. 6.5. Выбор элементов реестра для выявления несоответствий

Щелкните кнопку **Поиск проблем**, чтобы запустить поиск несоответствий в реестре.

В окне утилиты отобразится список найденных проблем в реестре (рис. 6.6).

Если вы не желаете исправлять какую-либо запись, то просто снимите соответствующий флажок в списке.

Теперь остается разрешить обнаруженные проблемы. Для этого щелк-ните кнопку **Исправить**. Вам будет предложено сохранить резервные копии сделанных изменений. Очень рекомендуем сделать это. Для этого выберите папку, куда будет помещен файл резервной копии. По умолчанию утилита создает имя файла из системной даты и времени.

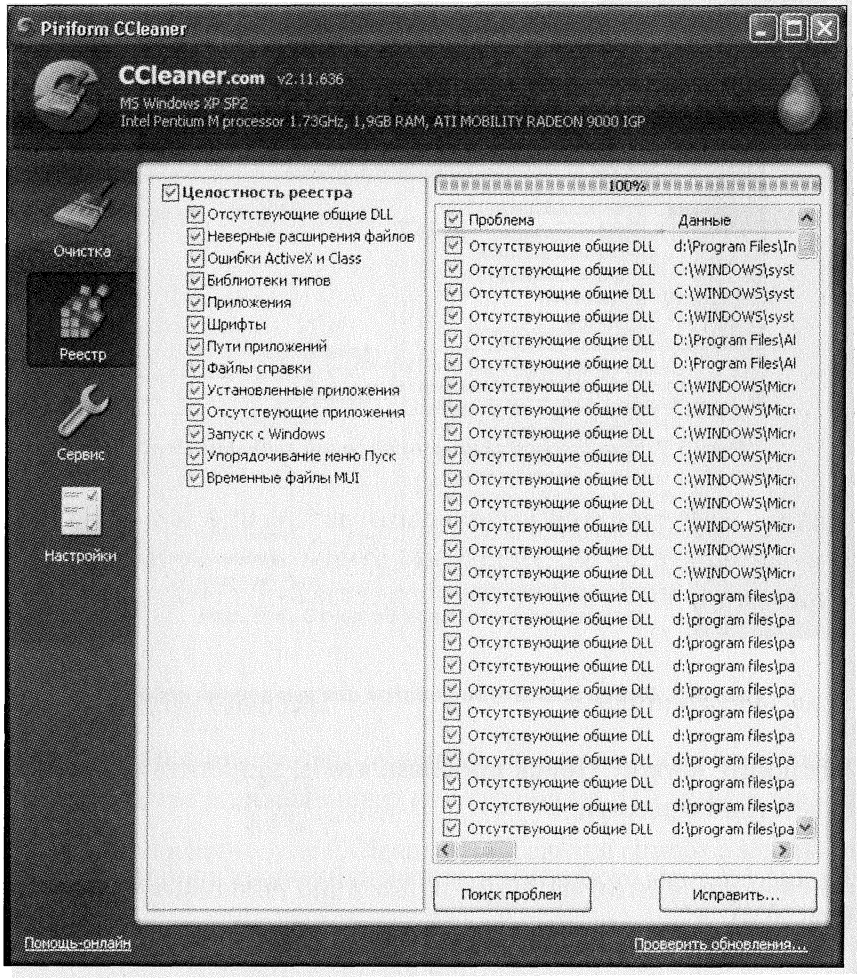


Рис. 6.6. Список обнаруженных несоответствий в реестре

Откроется диалоговое окно исправления проблемных значений реестра (рис. 6.7).

CCleaner предлагает вам удалять значения по отдельности или же все отмеченные флажками сразу. Здесь, конечно, выбор за вами, но при огромном списке несоответствий раздельное удаление может занять значительное время. Тем более что в экстренных слу-

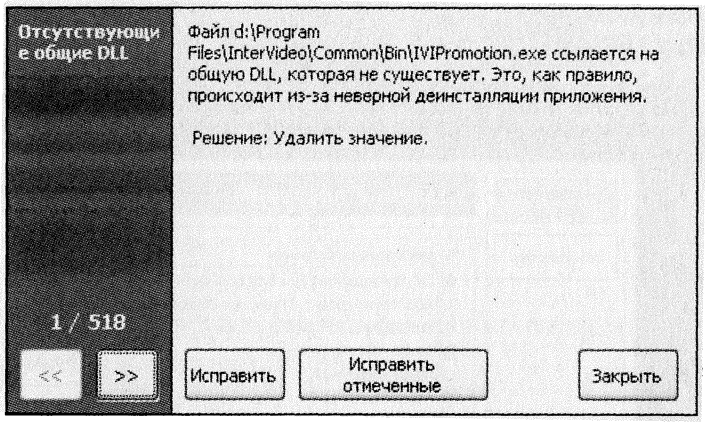


Рис. 6.7. Диалоговое окно исправления значений реестра

чаях мы всегда сможем восстановить потерянные значения. Поэтому щелкните кнопку **Исправить отмеченное**. За считанные секунды все проблемные элементы реестра будут исправлены.

Удаление приложений

Здесь вы можете деинсталлировать программы, а также управлять их автозапуском. Щелкните значок 

В окне утилиты отобразится список установленных на вашем компьютере приложений (рис. 6.8).

Справа от списка расположены четыре кнопки:

- **Деинсталляция**. Данная функция предназначена для полного удаления выбранного приложения с жесткого диска. Она аналогична стандартной деинсталляции программ с помощью стандартного средства Windows **Установка и удаление программ**.

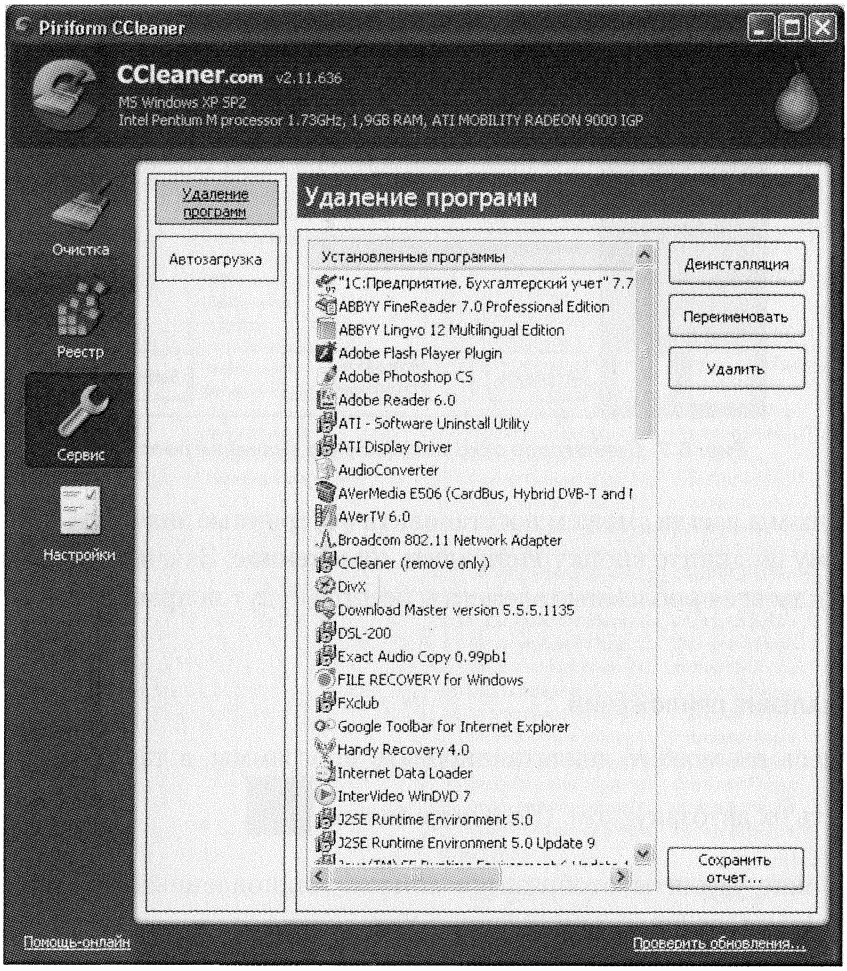


Рис. 6.8. Список программ, установленных на компьютере

- **Переименовать**. Здесь происходит переименование названия программы в списке приложений. При этом свойства самой программы останутся без изменений.

- **Удалить**. При выборе этой команды произойдет удаление записи о деинсталляции выбранной программы из реестра. При

этом само приложение не пострадает и будет функционировать, как и прежде.

- **Сохранить отчет**. Создает и сохраняет отчет о проделанных операциях с программами в выбранную вами папку.

Настройки

Данная часть CCleaner предназначена для пользовательской настройки различных функций программы.

Щелкните значок  и затем кнопку **Настройки**. Откроется диалоговое окно с общими настройками программы (рис. 6.9).

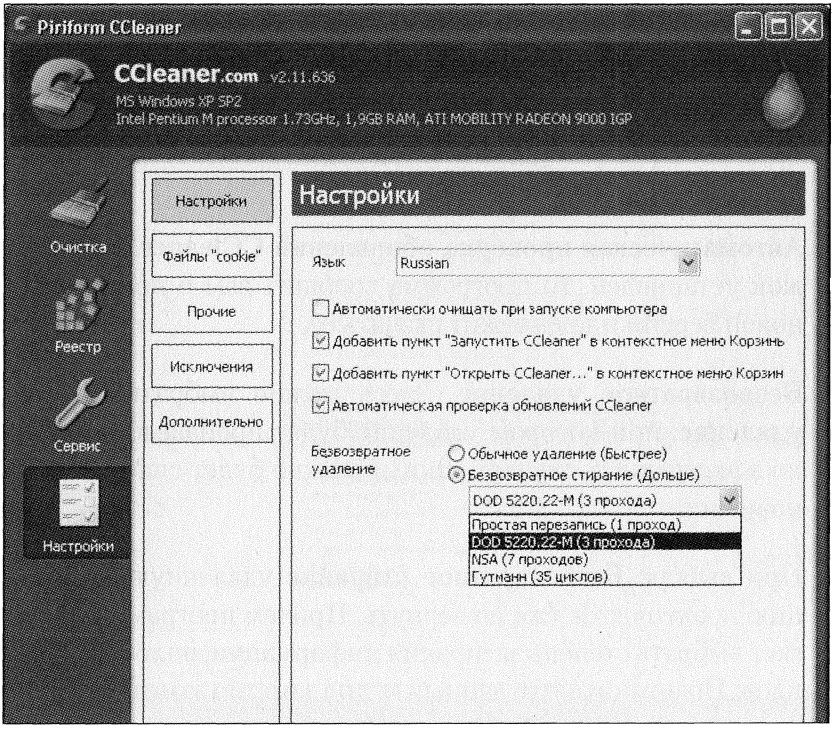


Рис. 6.9. Общие настройки CCleaner

Здесь вы можете изменить язык интерфейса утилиты на любой из доступных.

- **Автоматически очищать при запуске компьютера**. Выбор данной опции позволит выполнять выбранные элементы Windows и сторонних программ каждый раз при запуске операционной системы. В данном случае ваш компьютер будет находиться постоянно в «очищенном» состоянии.

- **Добавить пункт «Запустить CCleaner» в контекстное меню Корзины**. При включении этой опции вы сможете начать процесс очистки элементов Windows и других программ, щелкнув правой кнопкой мыши по Корзине и выбрав соответствующий пункт меню.

- **Добавить пункт «Открыть CCleaner...» в контекстное меню Корзины.** При включении этой опции вы сможете открыть утилиту CCleaner, щелк-нув правой кнопкой мыши по Корзине и выбрав данный пункт меню.

- **Автоматическая проверка обновлений CCleaner**. Если флажок установлен, то программа сообщит вам о появлении её новой версии и предложит скачать её.

- **Безвозвратное удаление**. Здесь можно выбрать **Обычное удаление**, при котором удаление будет произведено быстро, но в экстренных случаях данные можно будет спасти, восстановив их.

- При выборе **Безвозвратное стирание** удаленную информацию практически уже не вернуть. Причем программа предлагает выбрать степень затирания информации, вплоть до 35 циклов. Но помните, что данный метод заметно замедлит выполнение процесса очистки. Данный выбор оправдан, если на ва-

шем компьютере хранится действительно секретная или ценная информация.

Файлы "cookies"

Щелкните одноименную кнопку. Откроется два окна **Cookies для удаления** и **Cookies для сохранения** (рис. 6.10).

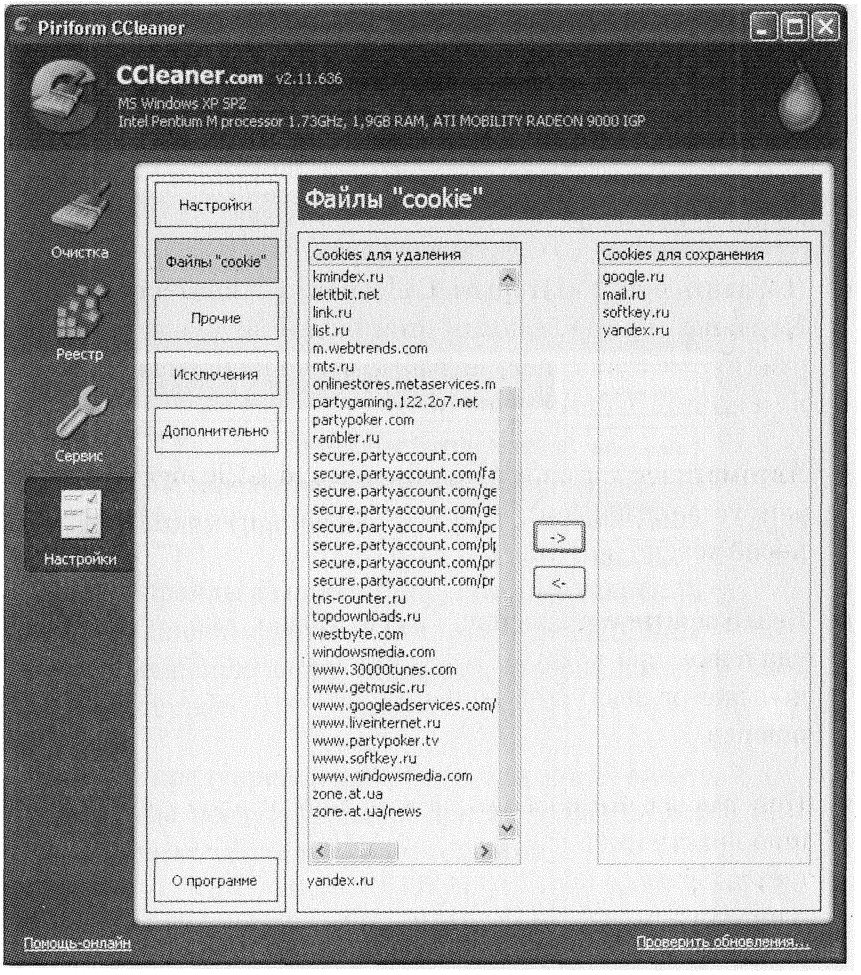


Рис. 6.10. Определение cookies, которые нельзя удалять

В первом окне отображается список cookies, которые будут удалены при выполнении операции удаления cookies (см. выше). Однако если вам необходимо, чтоб определенные cookies всегда оставались «живыми», то перенесите их из левого окна в правое с помощью стрелок. Если когда-нибудь они вам будут уже не нужны, то отправьте их обратно в список «смертников».

Прочие

В данном пункте Настроек можно удалять выбранные файлы (рис. 6.11).

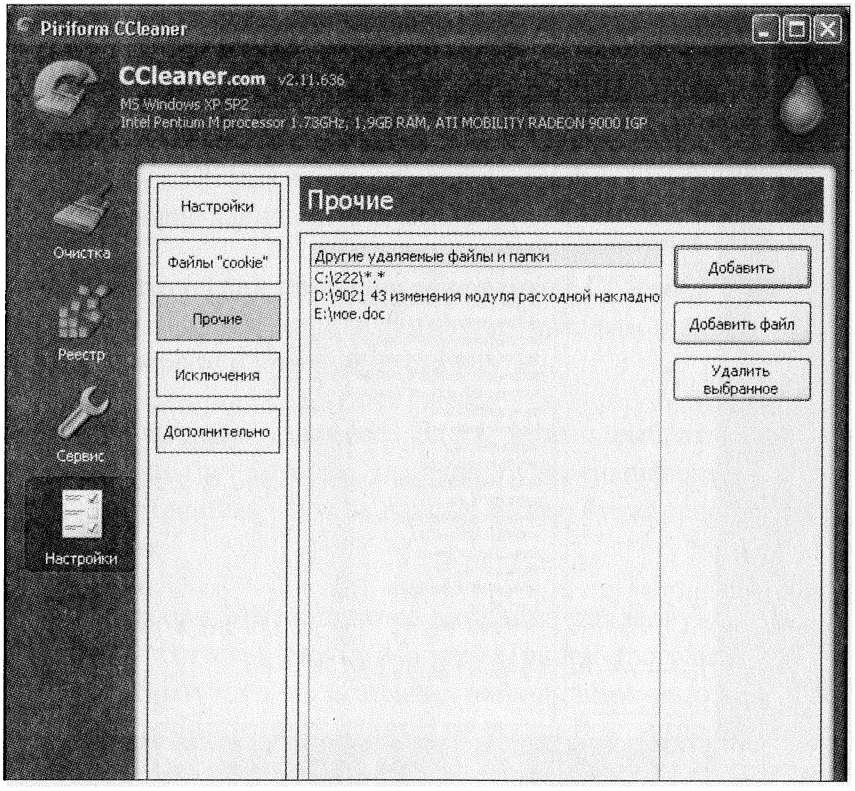


Рис. 6.11. Выбор объектов для удаления

Причем можно выбирать их как по одному, с помощью кнопки **Добавить файл,** так и целой папкой. Для этого нужно щелкнуть кнопку **Добавить** и выбрать нужную папку. Стоить отметить, что все файлы, находящиеся в выбранной папке, исчезнут, но сама папка почему-то останется целой и невредимой.

Если вы вдруг вспомните, что какие-то файлы вам все-таки милы, можно их убрать из списка «смертников» с помощью кнопки **Удалить выбранное**.

Исключения

Этот пункт является прямой противоположностью предыдущего. Здесь выбираются папки и файлы, которые, наоборот, не должны подлежать удалению ни при каких условиях. Кроме того, в список можно включать элементы реестра.

Дополнительно

Этот пункт настроек программы предназначен для выбора дополнительных опций (рис. 6.12).

- **Удалить файлы из папки Temp, которые старее 48 часов**. При выборе данной функции утилита будет автоматически очищать временную папку от файлов, которые находятся там более двух суток.

- **Скрыть предупреждения**. Если вам когда-нибудь надоедят различные предупреждения при выполнении той или иной операции, то установите здесь флажок.

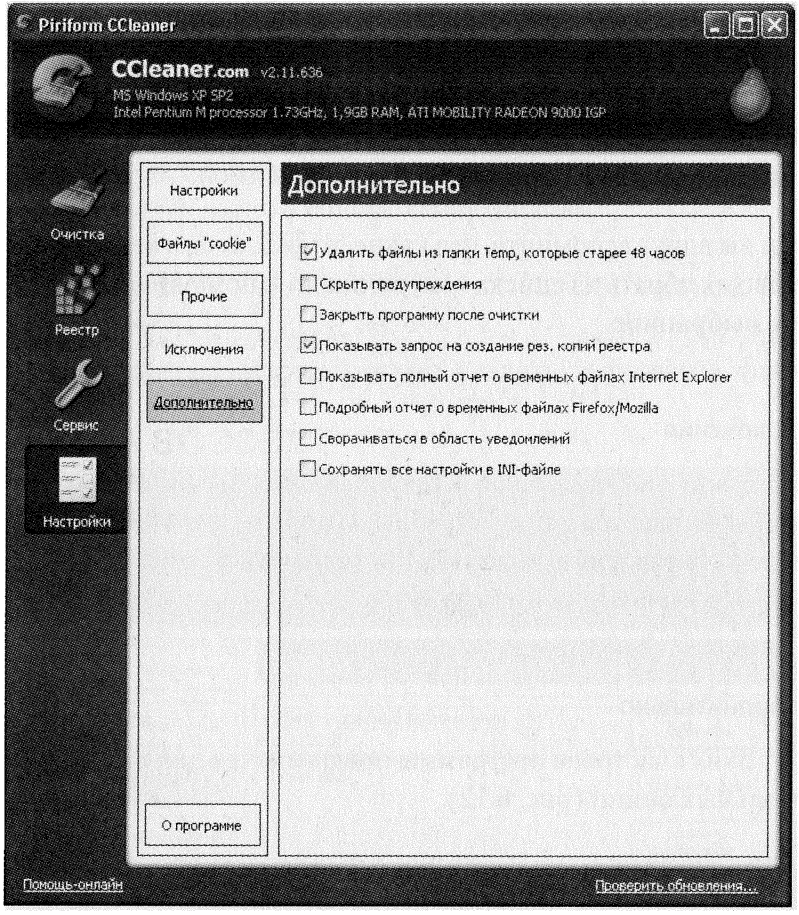
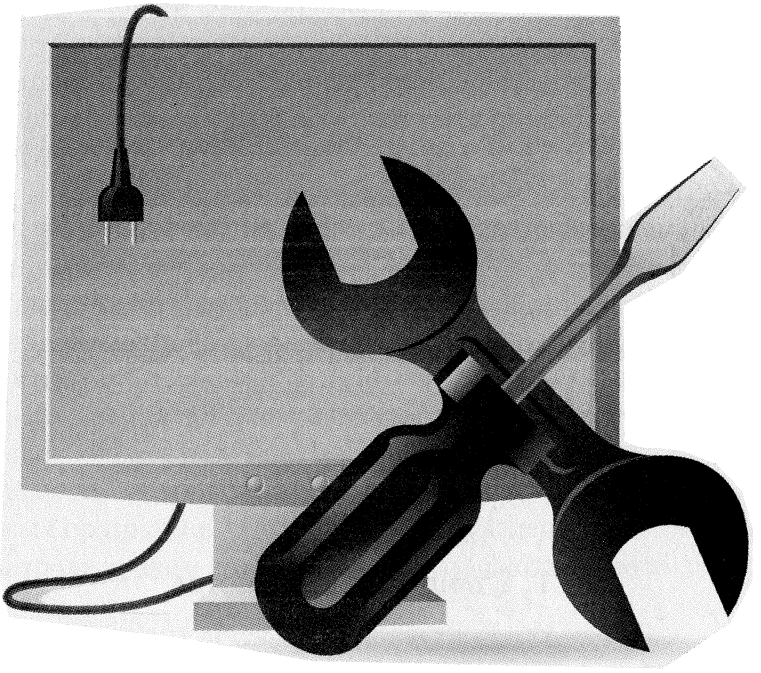


Рис. 6.12. Дополнительные настройки CCleaner

ГЛАВА 7.

ИЗБАВЛЯЕМСЯ ОТ АВТОМАТИЧЕСКОГО ЗАПУСКА НЕЖЕЛАТЕЛЬНЫХ ПРОГРАММ, «ВИСНУЩИХ» ПРОГРАММ И «ПЛОХИХ» ПРОЦЕССОВ



7.1. Контроль за автозагружаемыми программами

При загрузке операционной системы запускаются и многие другие программы, работающие в фоновом режиме. Фоновый режим подразумевает, что программы постоянно находятся в состоянии готовности или в рабочем состоянии, но не видны пользователю. Они выходят на передний план только при непосредственном обращении к ним.

Важность умения настраивать перечень автозагружаемых программ подкрепляется, во-первых, необходимостью контролировать, что у вас происходит в системе, во-вторых, грамотным расходованием ресурсов компьютера (если много программ будет запущено в фоновом режиме – компьютер начнет «тормозить»), а в-третьих, необходимостью исключения потенциально опасных программ из списка автоматически загружаемых.

7.1.1. Стандартные средства

В Windows XP

В Windows XP для того, чтобы та или иная программа или документ автоматически запускалась при загрузке системы, необхо-

димо добавить ее ярлык в меню «Пуск», в раздел **Все программы → Автозагрузка** (рис. 7.1). Делается это перетаскиванием. Соответственно, чтобы она не запускалась, необходимо исключить ее ярлык из указанного пункта главного меню.

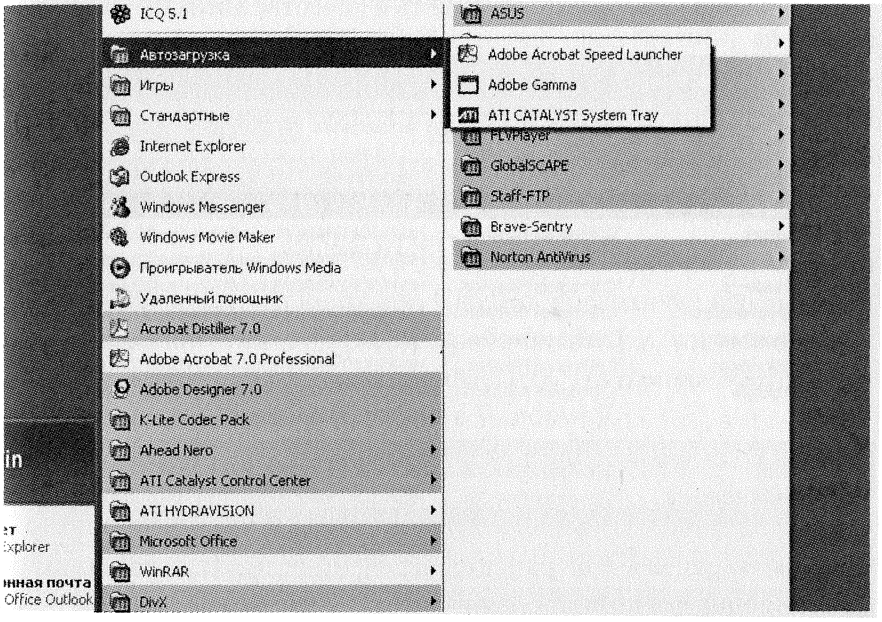


Рис. 7.1. Пункт «Автозагрузка» в Главном меню Windows

Все бы было хорошо, но в разделе **Автозагрузка** меню «Пуск» указывается примерно десятая часть программ, подлежащих автозагрузке. Поэтому ее удобнее использовать для ДОБАВЛЕНИЯ новых программ в автозагрузку. Для удаления и вообще лучшего контроля за этим делом следует пользоваться другим средством:

1. Выберите **Пуск → Выполнить**.

2. В появившемся окне Запуск программы введите **msconfig.exe** и нажмите «Enter».

3. В результате перед вами появится окно **Настройка системы**, на вкладке **Автозагрузка** которого вы и сможете откорректировать список автозапускаемых программ (см. рис. 7.2). Просто снимите галочки напротив тех программ, которые вы не хотите видеть в качестве автозагружаемых.

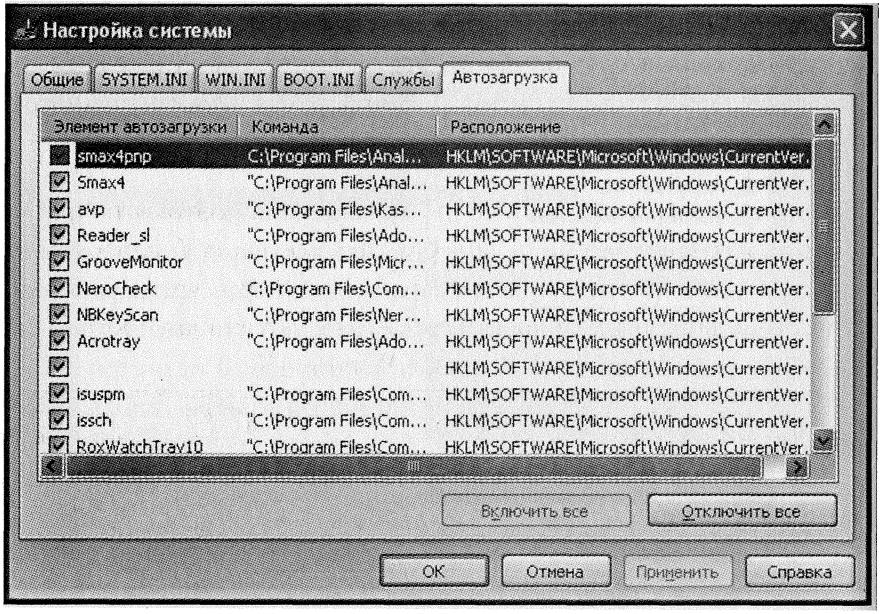


Рис. 7.2. Окно «Настройка системы». Вкладка «Автозагрузка»

В Windows 7 и в Windows 8

В Windows 7 все делается аналогично тому, как это происходит в Windows XP (см. выше).

7.1.2. С помощью специальных программ

Гораздо удобнее разбираться со списком автозагрузки с помощью специальных программ. Хотелось бы отметить программку, специально ориентированную на контроль автозагрузки, и облада-

ющую гораздо более «продвинутыми» возможностями. Имя ее – EF StartUp Manager (см. рис. 7.3).

EF StartUp Manager предназначена для управления приложениями, которые запускаются вместе с Windows. Программа дает возможность просматривать список таких приложений, временно отключать их, удалять и добавлять новые. Кроме этого, есть возможность определять порядок загрузки приложений и устанавливать задержку между ними. EF StartUp Manager имеет многоязычный интерфейс и поддерживает русский язык.

Работа с программой достаточно тривиальна, поэтому подробно мы рассматривать ее не будем. Скачать последнюю версию программы можно с сайта фирмы-разрабочика http://www.efsoftware.com. В заключение хотелось бы отметить, что данная программка работает как с Windows XP, так и с Windows 7.

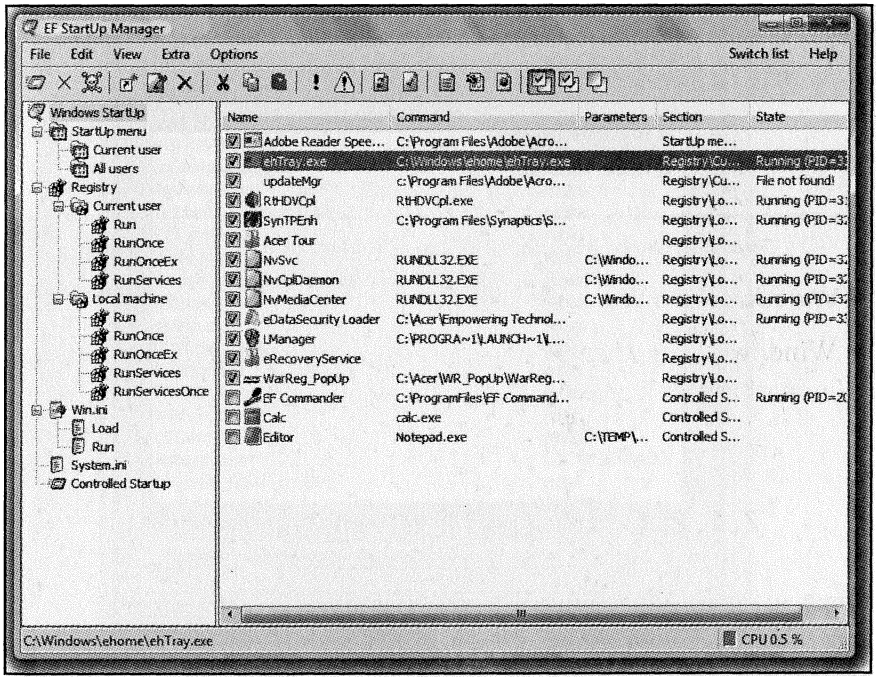


Рис. 7.3. Программа EF StartUp Manager

7.2. Контроль за происходящими в системе процессами. Диспетчер задач

Использование Диспетчера задач

В Windows предусмотрено средство мониторинга (и контроля) работы системы, позволяющее вам контролировать работу системы и выполняемые действия в системе. Это средство называется Диспетчером задач и присутствует как в Windows XP, так и в Windows 7. Вызвать его можно, нажав на три клавиши «Ctrl» + «Alt» + «Del». При этом вы либо сразу попадете в окно Диспетчера, либо перед этим отобразится окно, в котором вам будет предложено нажать кнопку Диспетчер задач, и уже после этого вы попадете в окно Диспетчера (см. рис. 7.4).

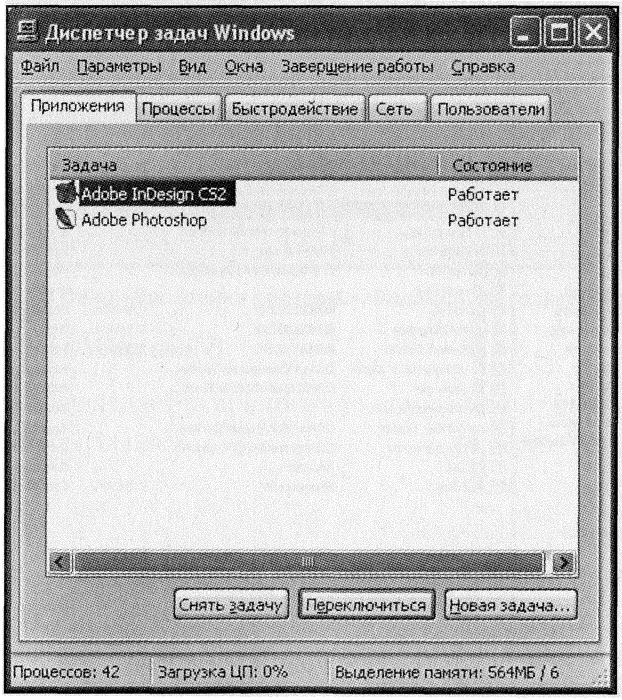


Рис. 7.4. Диспетчер задач. Вкладка «Приложения»

В окне Диспетчера задач, на вкладке **Приложения** (рис. 7.4) вы можете видеть и контролировать работу запущенных приложений. Это может быть особенно полезно, если приложение не отвечает на запросы (зависло) или работает в фоновом режиме и доступ к нему затруднен.

На вкладке **Приложения** вы можете увидеть полный список запущенных приложений и в случае необходимости прервать работу любого из них. Для этого следует выделить его в списке и нажать на кнопку **Снять задачу**.

Перейдя на вкладку **Процессы** окна Диспетчера задач (рис. 7.5), вы сможете получить список всех запущенных процессов в системе. При этом напротив каждого из них будет указана в процентах

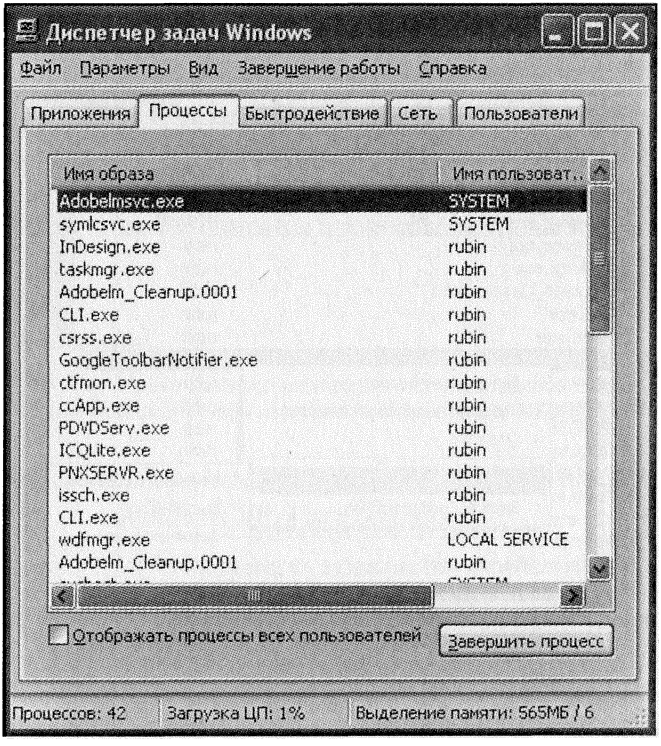


***Рис. 7.5. Вкладка* «Процессы»**

нагрузка приложения на процессор и систему, занимаемая процессом в данный момент.

Все, что происходит в системе, происходит в виде процессов. При этом программы запускаются также в виде процессов. Но, помимо программ, в системе работают еще и службы и прочие внутренние программы. Поэтому список процессов гораздо больше списка запущенных программ.

Кроме того, иногда в системе запускаются процессы без вашего ведома и разрешения. Поэтому рекомендуется периодически проверять запущенные в системе процессы и отключать непонятные и ненужные. Но делать последнее можно, только ясно себе

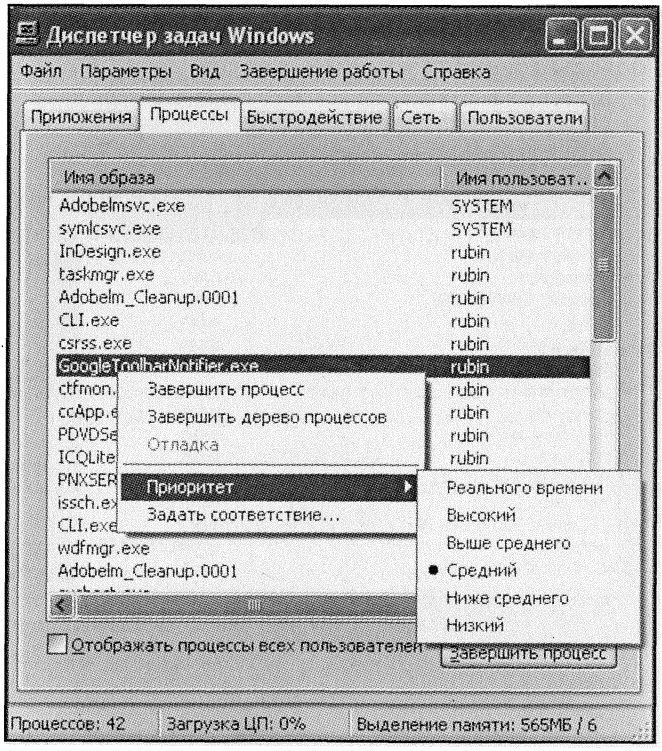


Рис. 7.6. Задаем приоритет процесса

представляя, что за процессы за что отвечают. Далее, в следующем пункте данной главы, приведено сводное описание системных процессов и процессов различных программ (в том числе и вредоносных).

Помимо всего прочего, вы можете на вкладке **Процессы** установить приоритет работы того или иного процесса. При этом процесс с большим приоритетом забирает под себя больше системных ресурсов (процессорного времени и пр.), а значит, и быстрее выполняется. Чтобы назначить приоритет процессу, следует щелкнуть по нему правой кнопкой мыши и в контекстном меню выбрать пункт **Приоритет**, а затем выбрать значение приоритета (рис. 7.6).

Какие процессы хорошие, а какие — плохие. Описание процессов

Далее, в табл. 7.1 приведено сводное описание процессов, которые можно наблюдать как в Windows XP, так и в Windows 7/Vista. Чуть ниже, в табл. 7.2 описаны процессы, встречающиеся только в Windows 7.

Примечание

При подготовке данного материала использовалась статья «Диспетчер, милый мой диспетчер» из журнала ComputerBild №24/2007

Таблица 7.1. *Сводное описание процессов, встречающихся в Windows XP/Vista/Windows 7*

Процесс	Что скрывается за процессом и что с этим делать
Accelerate.exe	Данный процесс принадлежит программе Internet Accelerator, используемой для увеличения скорости работы в Интернете. Соответственно, процесс не опасен, а его завершение приведет к завершению работы Internet Accelerator'а

Activation.exe	Процесс, соответствующий процедуре активации, предусмотренной в Windows XP, Vista, Windows 7 (возможно, и других программных продуктов Microsoft). Появляется только в моменты проведения активации и опасности не представляет
ACS.exe	Процесс служебной программы Atheros Configuration Service, отвечающей за соединение с беспроводной сетью. Опасности не представляет. Завершение процесса приводит к закрытию программы (вы не сможете пользоваться беспроводной сетью)
Adobes.exe	Процесс троянской программы FLOOD.BA, маскирующегося под процесс программы от Adobe. Представляет опасность. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
adobe_gamma_loader.exe	Процесс программы Gamma Loader отвечающей за корректное отображение цветов в программах от компании Adobe (в Фотошопе и т.д.). Однако иногда под этим именем «проходит» вредоносная программа. Так что желательно проверить наличие самой программы Gamma Loader у вас на компьютере. Сделать это можно, посетив папку C:\Programms\Common Files\ Adobe. В случае необходимости примите меры
adstatserv.exe	Процесс вредоносной программы, подменяющей стартовую страницу в браузере и внедряющегося в него. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
alcmtr.exe	Процесс-компонент драйвера для Realtek AC 97 и звуковых карт, поддерживающих формат HD-Audio. Завершение процесса приводит к завершению работы компонента (может «исчезнуть» звук). Опасности не представляет

Alert.exe	Процесс, соответствующий программе контроля материнской платы от компании MSI. Опасности не представляет
alg.exe	Процесс, соответствующий компоненту Application Layer Gateway, используемому брандмауэром Windows в своей работе. Опасности не представляет. Завершение работы приведет к невозможности корректной работы брандмауэра
ati2evxx.exe, atitask.exe, atiptaxx.exe	Процессы программ-настройщиков видеокарт от компании ATI. Их завершение отключит инструменты управления работой видеокарты. Опасности не представляют
Bargains.exe, bargain.exe	Процессы вредоносных программ-троянов, записывающих адреса посещаемых вами веб-страниц и передающих их злоумышленнику. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
Belt.exe	Вредоносная программа A better Internet, скачивающая и показывающая в браузере различную рекламу и изменяющая настройки браузера. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
bcmntray.exe	Данный процесс соответствует драйверу сетевых плат от компании Broadcomm. Отключать его не рекомендуется, так как это приведет к невозможности сетевого взаимодействия. Опасности не представляет
bitlord.exe	Данный процесс программы взаимодействия с пиринговой сетью BitTorrent Client. Опасности не представляет
Blank.exe	Процесс вредоносной программы. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой

bot.exe	Процесс вредоносной программы, устанавливающей новую стартовую страницу (без возможности изменения) и отключающей настройки безопасности браузера. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
btmon2.exe	Процесс программы-драйвера Bluetooth-соединения в ноутбуках Toshiba. Опасности не представляет. Завершение процесса приводит к невозможности использования Bluetooth-устройств
bttray.exe	Процесс программы-драйвера Bluetooth-соединения. Опасности не представляет. Завершение процесса приводит к невозможности использования Bluetooth-устройств
Buddy.exe	Вредоносная программа, отслеживающая ваши действия в Интернете и показывающая вам рекламу в виде всплывающих окон. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
bvt.exe	Процесс очень зловредного сетевого червя. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
Camdetekt.exe	Процесс, относящийся к работе программы-просмотрщику цифровых изображений ACDSee. Опасности не представляет
cd_instal.exe	Вредоносная программа от компании Cydoor Desktop Media. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
chkdsk.exe	Процесс, соответствующий стандартной программе сканирования/проверки дисков, встроенной в Windows. Однако, если вы подобную проверку не запускали, под маской данного процесса может быть запущена вредоносная программа. Будьте бдительны

CLI.exe	Процесс программы-настройщика видеокарт от компании ATI. Его завершение отключит инструменты управления работой видеокарты. Опасности не представляет
clipsvr.exe	Процесс, отвечающий за работу буфера обмена и появляющийся при копировании пользователем файла или текста в буфер обмена. Не рекомендуется ничего делать с этим процессом
cmd.exe	Процесс режима командной строки Windows. Если у вас командная строка не запущена, то значит – это вирус
CMDLineExt.dll	Процесс программной защиты от копирования, сопровождающий установку некоторых игр (например F.E.A.R). Отключение процесса возможно сделает невозможным играть в соответствующую игру. Опасности не представляет
comcfg.exe	Вредоносная программа. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
Command.exe	Процесс, имитирующий деятельность стандартной программы command.exe. Однако в большинстве случаев – это вирус
ctfmon.exe	Процесс одного из компонентов Microsoft Office, отвечающий за распознавание языков и шрифтов. Опасности не представляет
desktop.exe	Процесс вредоносной программы
ddhelp.exe	Процесс программного модуля, отвечающего за 3D-графику в играх. Опасности не представляет. Не рекомендуется трогать его
detektor.exe	Процесс, инициируемый многими программами для контроля за USB-разъемами. Опасности не представляет, но можно и отключить его.

devldr.32.exe	Процесс драйвера звуковых карт CreativeLabs. Опасности не представляет. Не рекомендуется его отключать, если вы не хотите отрубить у себя звук
DFrgNtfs.exe	Процесс программы дефрагментации жесткого диска. Опасности не представляет
directxset.exe	Вредоносная программа, маскирующаяся под программный драйвер DirectX. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
divx.exe	Вредоносная программа, маскирующаяся под известный видеокодек DivX. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
dlg.exe	Процесс, используемый при создании интернет-соединения через модем. Опасности не представляет. Завершать не рекомендуется
DllHost.exe	Системный процесс. Опасности не представляет. Завершать не рекомендуется
download.exe, downloadplus.exe	Вредоносные программы
druid_cchoice.exe	Процесс вредоносной троянской программы Generic2. UTD, распространяющейся обычно через электронную почту. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
Dumpprex.exe	Системный процесс, используемый службой отчета об ошибках Windows, которая отправляет техническую информацию о сбоях в работе программ компании Microsoft. Опасности не представляет. Можете завершить данный процесс, если никакие отчеты отправлять вы не собираетесь

DW20.exe	Процесс, отсылающий ошибки в работе программ Microsoft Office. Опасности не представляет. Однако, можете его отключить
eEBSVC.exe	Процесс проверки количества тонера в принтерах Epson и поиска новых драйверов в Интернете для вашего принтера. Опасности не представляет
eraseme_75103.exe	Вредоносная программа
eventmgr.exe	Процесс, относящийся к работе сканера. Опасности не представляет. Отключать не рекомендуется (сканер будет некорректно работать)
explorer.exe	Процесс оболочки Windows (Проводника). Однако возможна подмена
Fan.exe	Процесс программы, осуществляющей мониторинг температуры внутри системного блока или корпуса ноутбука. Опасности не представляет
faxsvc.exe	Процесс стандартной программы работы с факсами, встроенной в Windows. Опасности не представляет
FVProtekt.exe	Процесс вредоносного сетевого червя, рассылающего себя по электронной почте всем абонентам, найденным в вашем списке контактов (если таковой есть). В любом случае рекомендуется немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
gearsec.exe	Процесс, используемый многими программами для для записи CD и DVD. Опасности не представляет. Отключать не рекомендуется
getright.exe	Процесс программы GetRight, предназначенной для ускорения скачивания файлов из Интернета. Опасности не представляет

grnt.exe	Вредоносная программа. Следует немедленно завершить этот процесс и установить/воспользоваться антивирусной программой
googledesktop.exe	Процесс Google Desktop – локального поисковика от Google. Опасности не представляет. Отключать или не отключать – смотрите сами
graph.exe	Процесс программного модуля, входящего в Microsoft Office и предназначенного для построения графиков и диаграмм в программах Office. Опасности не представляет. Отключать не рекомендуется
HelpCtr.exe, HelpHost.exe	Процессы справочных систем Windows. Опасности не представляет. Отключать не рекомендуется
helpexp.exe	Вредоносная программа
hh.exe	Процесс, отображающий файлы помощи. Опасности не представляет
hidden.exe, hidden32.exe	Вредоносные программы
hidserv.exe	Процесс программы-драйвера, обеспечивающей воспроизведение звука звуковыми картами, подключенными через USB-разъем. Опасности не представляет. Отключать не рекомендуется
icq.exe	Процесс известного мессенджера ICQ-клиента (Аськи). Опасности не представляет. Отключение приводит к закрытию аськи
iexplore.exe	Процесс, соответствующий браузеру Internet Explorer. Опасности не представляет. Отключать не рекомендуется (если вы, конечно, не хотите закрыть все окна браузера)
imapi.exe	Процесс, обеспечивающий многим программам функции записи CD . Опасности не представляет. Отключать не рекомендуется
isass.exe (lsass.exe)	Вредоносные программы

java.exe, javaw.exe, javaws.exe	Процессы виртуальной Java-машины, предназначенной для корректного отображения Java-апплетов на Интернет-страницах. . Опасности не представляет. Отключать не рекомендуется
kernel32.exe	Вредоносная программа, маскирующаяся под процесс ядра Windows
keylogger.exe	Вредоносная программа
keyrngr.exe	Вредоносная программа
ledriver.exe	Вредоносная программа
LifeExp.exe	Процесс, используемый веб-камерой Microsoft Lifecam для своей работы. Опасности не представляет. Отключать не рекомендуется
loadwc.exe	Процесс, соответствующий программе Web Check – модулю Internet Explorer. Опасности не представляет. Можно отключить
locator.exe	Процесс Microsoft Locator, используемый некоторыми сетевыми функциями. Опасности не представляет. Отключать не рекомендуется
lsa.exe	Вредоносная программа, маскирующаяся под обычный процесс Local Security Authority
LSSrvc.exe	Процесс, запускающийся вместе с Nero и отвечающий за возможности прожига на поверхности спец. дисков различных изображений (реализует технологию LightScribe). Опасности не представляет. Отключать не рекомендуется
Microsoft.exe	Вредоносная программа GAOBOT
mscache.exe	Вредоносная программа
msoobe.exe	Процесс, соответствующий процедуре активации Microsoft-Out-of-Box-Experience для продуктов Windows. Опасности не представляет. Отключать не рекомендуется

MSUpdate.exe	Вредоносная программа, маскирующаяся под программу обновления Windows
mapisp32.exe	Служебный процесс, используемый некоторыми программами Microsoft. Опасности не представляет. Отключать не рекомендуется
Mixer.exe	Процесс, отвечающий за управление звуковыми картами производства C-Media. Опасности не представляет. Можно отключить
Moviemk.exe	Процесс стандартной программы обработки видео Windows Movie Maker, входящей в состав Windows. Опасности не представляет. Отключение процесса приводит к завершению работы программы
MSWheel.exe	Служебный процесс программы Microsoft Intellipoint, предназначенной для настройки мыши и клавиатуры. Опасности не представляет. Отключать не рекомендуется
NavPass.exe	Вредоносная программа, скачивающая на ваш компьютер всевозможные вирусы
NsUpdate.exe	Вредоносная программа, пытающаяся дозвониться через модем на различные платные номера телефонов (порнографических ресурсов)
nerocheck.exe	Процесс, препятствующий блокировке программой Nero других программ для записи дисков. Опасности не представляет. Отключать не рекомендуется
notepad.exe	Процесс текстового редактора Блокнот. Если Блокнот у вас не запущен – то это вирус
nsvclog.exe	Процесс мониторинга видеокарт Nvidia Service Log, фиксирующий проблемы в работе видеокарты от NVidia. Опасности не представляет. Можно отключить
ocvdll.exe	Вредоносная программа

olehelp.exe	Вредоносная программа
osd.exe	Процесс On-Screen Display, предназначенный для отображения на экране текстов большого объема Опасности не представляет. Отключать не рекомендуется
patch.exe	Скорее всего, это вредоносная программа
qtask.exe	Процесс, осуществляющий быстрый доступ к функциям Quicktime. Опасности не представляет. Имеет смысл отключить, если вы не используете Quicktime
quickres.exe	Процесс небольшой утилиты смены разрешения экрана монитора, разработанной самой корпорацией Microsoft. Опасности не представляет. Имеет смысл отключить, если вы не пользуетесь данной утилитой
rapimgr.exe	Процесс программы Microsoft ActiveSync, ответственной за синхронизацию с карманными компьютерами и другими мобильными устройствами. Опасности не представляет
regedit.exe	Процесс редактор реестра. Однако под него может маскироваться какая-либо вредоносная программа
RunDLL32.exe	Системный процесс Windows, без которого не работает большинство программ. Опасности не представляет. Отключать не рекомендуется
safe.exe. safenow.exe	Вредоносная программа
scm.exe	Процесс службы Service Control Manager, отвечающей за работу других служб Windows. Опасности не представляет. Отключать не рекомендуется
SearchNav.exe	Вредоносная программа, ворующая ваши конфиденциальные данные
services.exe	Системный процесс Windows (очень важный). Опасности не представляет. Отключать не рекомендуется

serviceS.exe	Вредоносная программа GAOBOT, маскирующаяся под системный процесс services.exe
sessmgr.exe	Системный процесс, используемый при дистанционном управлении компьютером. Опасности не представляет. Если дистанционного управления не предполагается, то рекомендуется процесс отключать
slsvc.exe	Процесс службы «Лицензирование программного обеспечения», отвечающей за воспроизведение защищенной от копирования музыки (WMA) и видеофайлов (WMV). Опасности не представляет. Отключение может привести к сложностям воспроизведения каких-либо видео- или музыкальных композиций
smss.exe	Процесс службы Session Manager Subsystem, «работающей» при входе и выходе пользователя из системы. Опасности не представляет. Отключать не рекомендуется
sp.exe	Вредоносная программа – клавиатурный шпион
staem.exe	Процесс, необходимый для запуска некоторых игр, например "Half Life" компании Valve. Опасности не представляет. Отключение приводит к невозможности запуска некоторых игр
svchost.exe	Служебный процесс Windows. Опасности не представляет. Отключать не рекомендуется. Но иногда этот процесс заражается вирусом
SysUtil.exe	Процесс, используемый для проверки подлинности программ. Опасности не представляет. Отключать не рекомендуется
Taskbar.exe	Вредоносная программа – червь W32.Frethem. Маскируется под процесс Диспетчера задач (см. ниже)
Taskmgr.exe	Процесс Диспетчера задач. Опасности не представляет. Отключать не рекомендуется

tcpsvcs.exe	Процесс, реализующий сетевые функции для некоторых программ. Опасности не представляет. Отключение может привести к осложнениям в сетевом взаимодействии
testing.exe	Вредоносная программа, повреждающая сетевые функции Windows
tmp.exe	Вредоносная программа
tsl.exe	Вредоносная программа Traveling Salesman, ворующая конфиденциальную информацию
tvm.exe	Вредоносная программа
twain_16.dll.exe	Вредоносная программа
Type32.exe	Процесс служебной программы Intellipoint, реализующей поддержку дополнительных функций мыши и клавиатуры. Опасности не представляет. Отключать не рекомендуется
UMonit2k.exe	Процесс, контролирующий USB-подключение карт-ридера. Опасности не представляет. Можно отключить, если вы не пользуетесь карт-ридером
uninst.exe	Системный процесс, запускаемый при удалении программного обеспечения. Если он активен постоянно – то это вирус
uninstall.exe	Системный процесс, запускаемый при удалении программного обеспечения. Если он активен постоянно – то это вирус
userinit.exe	Процесс программы, открывающей Рабочий стол и активирующей сетевые функции после запуска Windows. Опасности не представляет. Отключать не рекомендуется
vmnetdhcp.exe	Процесс, относящийся к работе виртуальной машины VMWare Workstation. Опасности не представляет. Отключать не рекомендуется
wab.exe	Процесс адресной книги Windows. Опасности не представляет. Отключать или не отключать – смотрите сами

wcescomm.exe	Процесс, отвечающий за синхронизацию данных с КПК. Опасности не представляет. Отключать не рекомендуется
wcmdmgr.exe	Процесс, который ищет и устанавливает обновления для аппаратных компонентов вашего ПК. Опасности не представляет. Отключать не рекомендуется
wdfmgr.exe	Системный процесс, присутствующий в Windows XP Service Pack 2 и связанный с оптимизацией работы драйверов. Опасности не представляет. Отключать не рекомендуется
wincomm.exe	Вредоносная программа
Windows.exe	Вредоносная программа, маскирующаяся под исполняемый файл Windows
winmgmt.exe	Важный системный процесс Windows, без которого не работают многие программы Опасности не представляет. Отключать не рекомендуется
WinRAR.exe	В принципе это процесс программы-архиватора WinRar. Однако очень часто под этим именем встречается вредоносная программа Coolwebsearch. Закройте архиватор и проверьте, завершится ли процесс
winxp.exe	Вредоносная программа
wow.exe	Процесс, обеспечивающий совместимость текущей версии Windows с программами, написанными для более ранних версий Windows. Опасности не представляет. Отключать не рекомендуется
wuauclt.exe	Процесс, отвечающий за скачивание и установку обновлений Windows из Интернета
xpservicepack.exe	Вредоносная программа

zone.exe	Процесс, реализующий многопользовательский режим во многих компьютерных играх от Microsoft (например, в Age of Empires), Опасности не представляет, но возможно его заражение

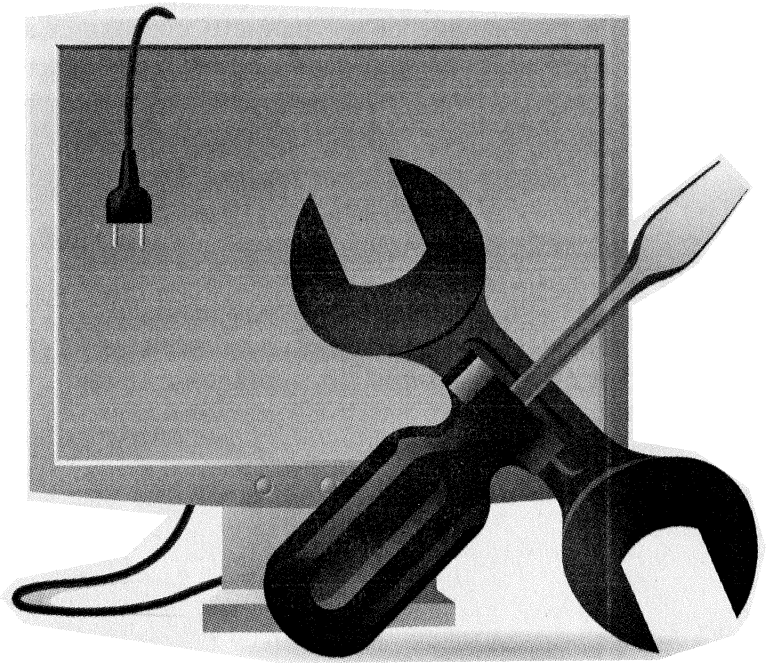
Таблица 7.2. *Процессы, относящиеся только к Windows 7*

audiodg.exe	Процесс, обеспечивающий корректную работу звуковой карты в Windows 7. Опасности не представляет. Отключать не рекомендуется
dwm.exe	Процесс модуля Desktop Windows Manager, отвечающего за трехмерные эффекты в Windows 7. Опасности не представляет. Отключать не рекомендуется
FXSSVX.exe	Процесс стандартной программы работы с факсами, встроенной в Windows 7. Опасности не представляет
LogonUI.exe	Процесс, предназначенный для входа в систему и удаленного управления через Интернет. Опасности не представляет. Отключать не рекомендуется
MSASCui.exe	Процесс Защитника Windows, встроенного в Windows 7. Опасности не представляет. Отключать не рекомендуется
sdclt.exe	Процесс, запускаемый при резервном копировании Windows 7. Опасности не представляет. Отключать не рекомендуется
Searchindexer.exe	Процесс, соответствующий модулю поиска в Windows 7. Опасности не представляет. Отключать не рекомендуется
Sidebar.exe	Процесс Боковой панели Windows 7. Опасности не представляет. Отключение процесса приводит к исчезновению Боковой панели с экрана
VSSvc.exe	Процесс, отвечающий за теневое копирование томов. Опасности не представляет. Отключать не рекомендуется

wercon.exe	Процесс, ответственный за отправку данных об ошибках в Microsoft. Опасности не представляет. Рекомендуется отключать
wmdc.exe	Процесс модуля Windows Mobile Device Center, отвечающего за синхронизацию файлов с КПК. Опасности не представляет. Отключать не рекомендуется
wpcumi.exe	Процесс, соответствующий функции родительского контроля, имеющейся в Windows 7. Опасности не представляет. Отключать не рекомендуется
WUDFHost.exe	Служебный процесс Windows 7, необходимый для корректной работы многих устройств. Опасности не представляет. Отключать не рекомендуется.

ГЛАВА 8.

В СИСТЕМЕ ПОСТОЯННЫЕ СБОИ И «ГЛЮКИ», WINDOWS ОТКАЗЫВАЕТСЯ РАБОТАТЬ. КАК ВОССТАНОВИТЬ РАБОТУ WINDOWS



8.1. Восстановление Windows XP

Восстановление Windows XP

Восстановить (сделать «откат» к стабильным настройкам) систему Windows XP очень просто. Для этого необходимо выполнить **Пуск →Все программы → Стандартные → Служебные → Восстановление системы**. После этого будет запущена программа **Мастер восстановления**.

В первом появившемся окне **Мастера восстановления** (см. рис. 8.1) выберите **Восстановление более раннего состояния компьютера** (он и выбран по умолчанию) и нажмите кнопку **Далее**.

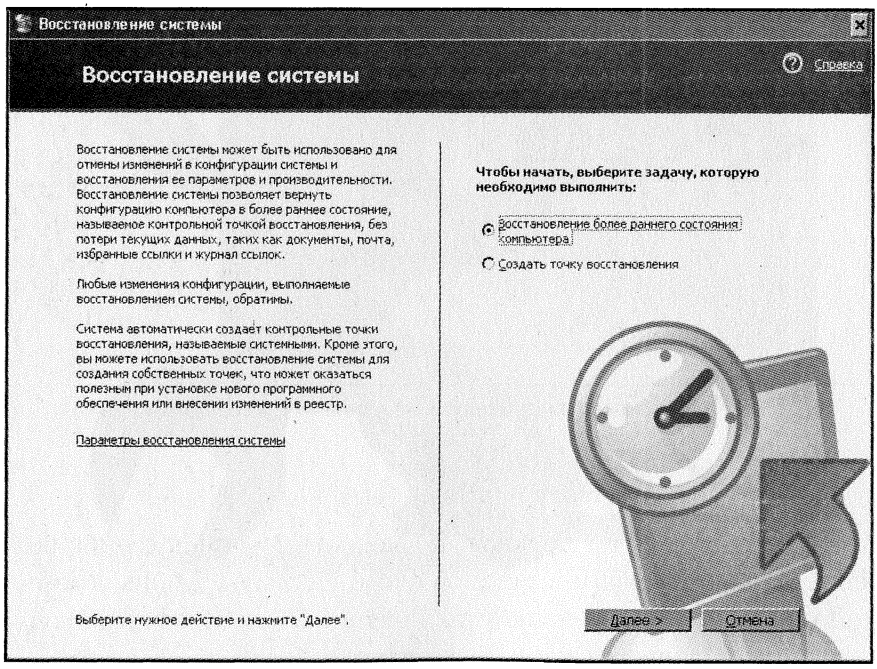


Рис. 8.1. Мастер восстановления: выбираем режим работы

После этого от вас в окне **Выбор точки восстановления** потребуется выбрать точку восстановления (см. рис. 8.2.). При этом будет показан интерактивный календарь, в котором надо выбрать дату, когда была создана точка восстановления. Такие даты отображаются жирным шрифтом. Одной дате могут соответствовать несколько точек восстановления. В этом случае одну точку из нескольких можно выбрать в расположенном рядом с календарем поле. Выбрав точку восстановления, нажмите **Далее**.

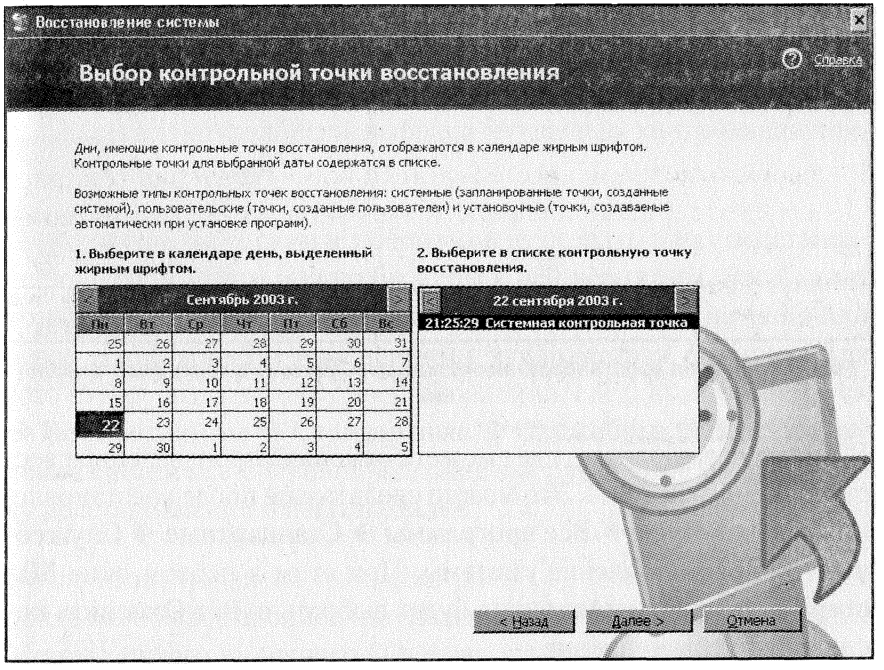


Рис. 8.2. Мастер восстановления: выбираем точку восстановления

После этого вам будет предложено закрыть все приложения, перед тем как произвести восстановление. Когда вы теперь нажмете **Далее**, будет запущено восстановление Windows XP. По окончании этого процесса (рис. 8.3.) компьютер будет перезагружен.

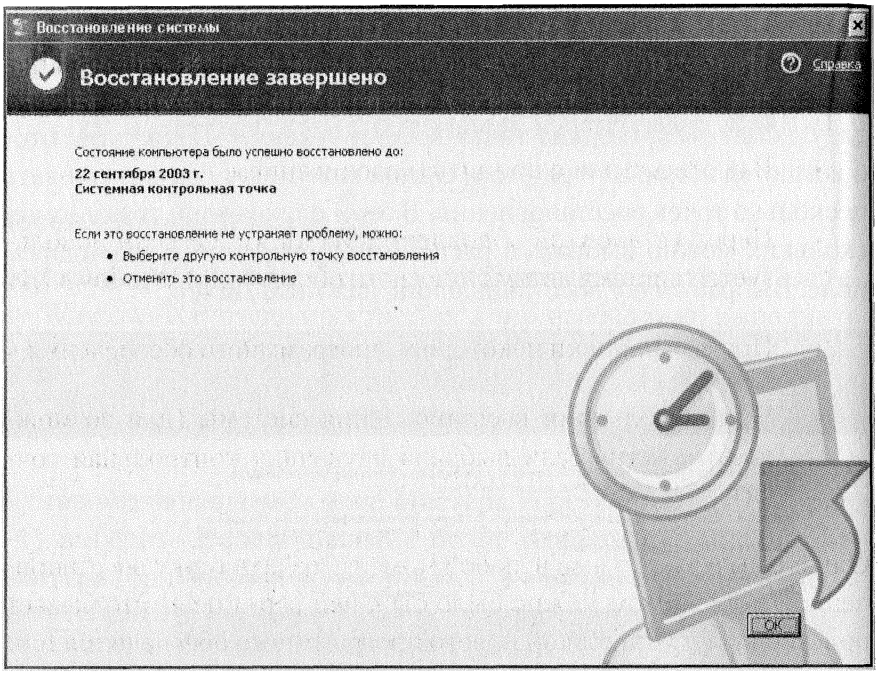


Рис. 8.3. Мастер восстановления: «откатили» Windows в точку восстановления

В случае необходимости вы можете отменить произведенное восстановление системы. Это можно сделать еще после восстановления, выбрав **Пуск ➔ Все программы ➔ Стандартные ➔ Служебные ➔ Восстановление системы**. При этом в первом окне **Мастера восстановления** можно будет выбрать пункт **Отменить последнее восстановление**.

Создание точек восстановления

Точки восстановления обычно автоматически создаются в следующих ситуациях:

- При первом запуске компьютера после обновления системы на Windows XP Professional.

- При установке нового драйвера, который не подписан и не сертифицирован организацией Windows Hardware Quality Labs (WHQL).
- В соответствии с принятым расписанием.
- Перед установкой обновлений Windows XP, если используется система автоматического обновления Windows XP.
- После установки некоторого программного обеспечения.
- При выполнении восстановления системы (для возможности отката, если выбрана неудачная контрольная точка).

Однако вы можете сами в любой момент создать точку восстановления, чтобы потом можно было бы к ней вернуться. Это бывает полезно перед установкой нового программного обеспечения или перед масштабными изменениями в параметрах системы. Для того чтобы создать точку восстановления, следует выбрать **Пуск → Все программы → Стандартные → Служебные → Восстановление системы**, в появившемся окне выбрать пункт **Создать точку** восстановления и нажать **Далее**.

После этого появится окно (см. рис. 8.4), в котором вам будет предложено ввести описание создаваемой точки восстановления. Можете ничего не вводить. Однако, чтобы потом не запутаться, для себя рекомендуется указать, что это за точка. Нажмите **Создать,** и точка восстановления будет создана. Закрывать все приложения при этом необязательно. Перезагрузка компьютера производиться не будет.

Существует еще возможность настройки регулярного создания точек восстановления, при котором эти точки будут создаваться автоматически через определенный промежуток времени. Но это делать

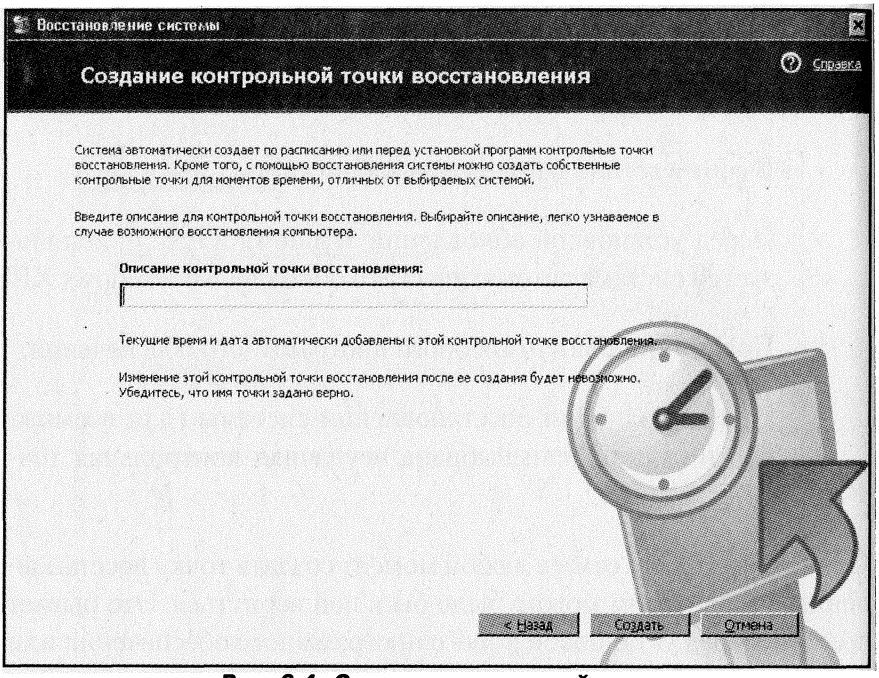


Рис. 8.4. Создание контрольной точки

не рекомендуется, так как «точка восстановления» занимает на жестком диске определенное место. Поэтому, создавая их регулярно по расписанию, вы можете быстро засорить свой жесткий диск. Создавайте точки восстановления только тогда, когда это действительно необходимо.

8.2. Восстановление Windows Vista

Процедура восстановления Windows Vista

Восстановить (сделать «откат» к стабильным настройкам) систему Windows Vista очень просто. Для этого необходимо выполнить **Пуск → Все программы → Стандартные → Служебные → Восстановление системы**. После этого будет запущена программа **Мастер восстановления**.

В первом появившемся окне (см. рис. 8.5) вам будет предложено либо откатиться к предлагаемой точке восстановления, либо самим выбрать точку восстановления.

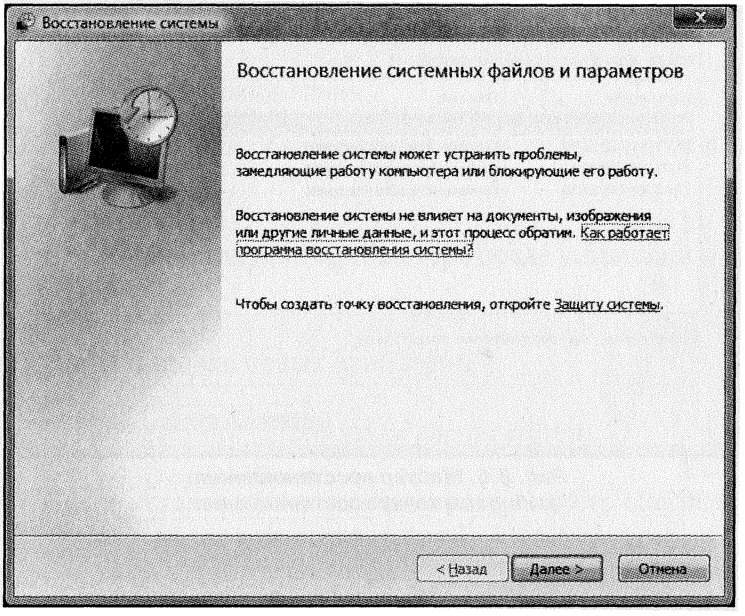


Рис. 8.5. Мастер восстановления: выбираем режим работы

Если вы захотите сами выбрать точку восстановления (рекомендуется), следует установить переключатель в соответствующее положение и нажать кнопку **Далее**. После этого от вас потребуется выбрать точку восстановления (см. рис. 8.6.). Выбрав точку восстановления, нажмите **Далее**.

После этого вам будет предложено закрыть все приложения, перед тем как произвести восстановление. Когда вы теперь нажмете **Далее**, будет запущено восстановление Windows Vista. По окончании этого процесса компьютер будет перезагружен.

В случае необходимости вы можете отменить произведенное восстановление системы. Это можно сделать еще после восстановле-

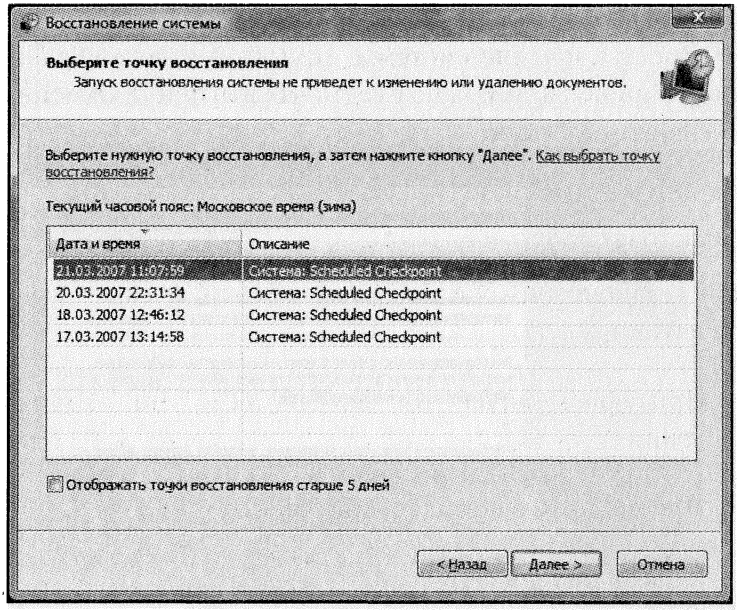


Рис. 8.6. Мастер восстановления: выбираем точку восстановления

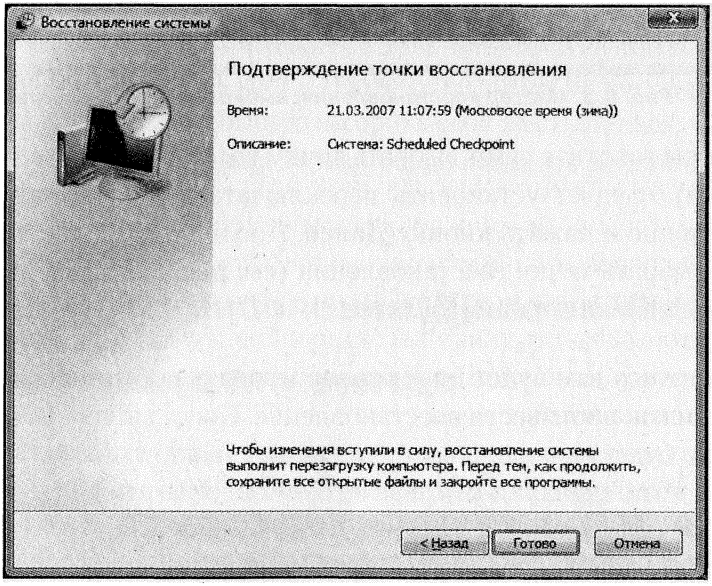


Рис. 8.7. За шаг до отката

ния, выбрав **Пуск → Все программы → Стандартные → Служебные → Восстановление системы**. При этом в первом окне **Мастера восстановления** можно будет выбрать пункт **Отменить последнее восстановление**.

Создание точек восстановления

Точки восстановления обычно автоматически создаются в следующих ситуациях:

- При первом запуске компьютера после установки и обновления.
- При установке новых драйверов.
- В соответствии с принятым расписанием.
- После установки некоторого программного обеспечения.
- При выполнении восстановления системы (для возможности отката, если выбрана неудачная контрольная точка).

Однако вы можете сами в любой момент создать точку восстановления, чтобы потом можно было бы к ней вернуться. Это бывает полезно перед установкой нового программного обеспечения или перед масштабными изменениями в параметрах системы. Для того чтобы создать точку восстановления, следует выбрать **Пуск → Панель управления → Система** и щелкнуть мышкой по задаче **Защита системы**.

Далее в появившемся диалоговом окне **Система** на вкладке **Защита** (см. рис. 8.8) вам будет предложено выбрать диск или диски, на которых следует создать точки восстановления, а затем – нажать кнопку **Создать**.

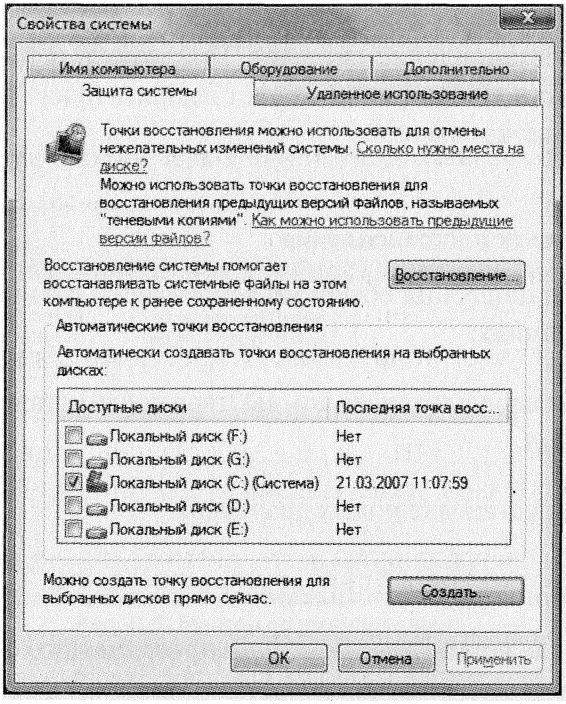


Рис. 8.8. Создание контрольной точки восстановления

После этого появится окно (см. рис. 8.9), в котором вам будет предложено ввести описание создаваемой точки восстановления. Можете ничего не вводить. Однако, чтобы потом не запутаться, для себя рекомендуется указать, что это за точка. Нажмите **Создать** — и точка восстановления будет создана. Закрывать все при-

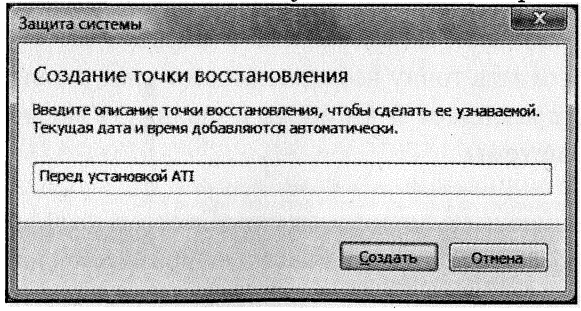


Рис. 8.9. Ввод названия контрольной точки

ложения при этом не обязательно. Перезагрузка компьютера производиться не будет.

8.3. Восстановление Windows 7

Само восстановление описано в п. 8.3.3., и вы можете сразу туда отправиться. Но сначала хотелось бы описать механизмы, которые позволяют сделать восстановление Windows 7 наиболее эффективным и действенным.

8.3.1. Резервное копирование и восстановление Windows 7

Windows 7 предоставляет своим пользователям мощные собственные инструменты, как для собственной защиты, так и для защиты пользовательских файлов.

Для защиты операционной системы как от различного рода сбоев, так и от вредительского вторжения в неё можно создать образ системы, который представляет собой точный образ диска. Восстановление компьютера из образа системы полное: нельзя выбрать отдельные объекты для восстановления, будут заменены все текущие программы, системные параметры и файлы.

Хотя образ системы и содержит абсолютно все файлы компьютера, ежедневное его создание будет занимать значительное время (особенно при огромном количестве информации). К тому же многие из сохраняемых в образ системы файлов вам и не нужны. Поэтому более регулярно рекомендуется создавать резервное копирование файлов. Программа архивации Windows позволяет создавать копии файлов данных для всех пользователей компьютера. Вы можете отдать системе право выбора объектов для резервного копирования или самостоятельно выбрать отдельные папки, библиотеки и диски для архивирования. Делать резервные копии можно как вручную, так и автоматически, по расписанию. Windows не выполняет создания копии всех установленных вами файлов, а лишь тех, которые изменились за этот период. Этим время архивирования заметно сокращается.

Кроме резервного копирования, Windows 7 имеет механизм автоматического сохранения копий файлов и папок. Предыдущие версии файлов можно использовать для восстановления случайно измененных, удаленных или поврежденных файлов и папок. Предыдущие версии могут оказаться полезными, однако они не равнозначны резервной копии, поскольку файлы заменяются новыми версиями и будут недоступны в случае сбоя диска.

Кроме перечисленных, в Windows 7 используется система восстановления с помощью точек (как и в предыдущих версиях), где можно отменить изменения, внесенные в систему компьютера, не затрагивая личные файлы, например электронную почту, документы или фотографии.

Чтобы создать резервную копию файлов либо образ системы, перейдите в **Панель управления** и выберите компонент **Архивация и Восстановление**. Откроется окно **Архивация и восстановление файлов** (рис. 8.10).

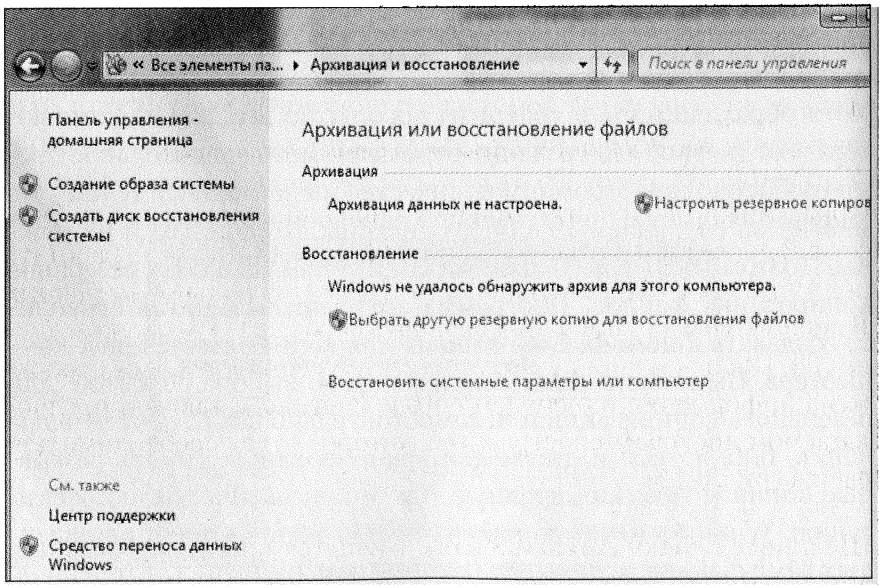


Рис. 8.10. Окно резервного копирования

Создание образа системы

Для создания образа системы щелкните одноименную ссылку (рис. 8.11).

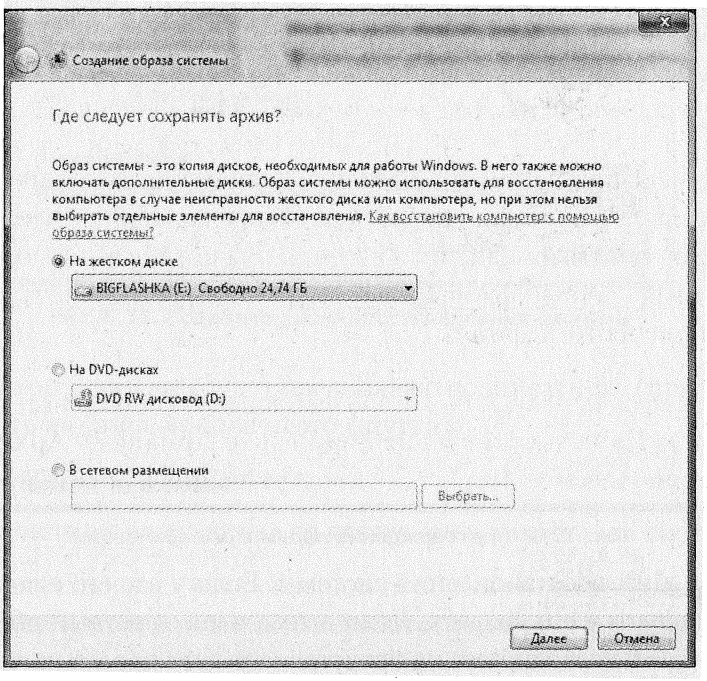


Рис. 8.11. Выбор хранилища для образа системы

Образ можно сохранить только на внешних носителях либо в сети. В последнем случае сохраняемый источник должен работать под Windows 7 Максимальной или Профессиональной редакции. В нашем примере мы будем сохранять образ на USB жестком диске (E). Щелкаем кнопку **Далее**. В следующем окне будет отображена информация о будущем образе системе, а также о предполагаемом дисковом пространстве, которое будет необходимо для файла (рис. 8.12).

Щелкните кнопку **Архивировать**. Начнется процесс сохранения архива. По его окончании на экране отобразится предложение

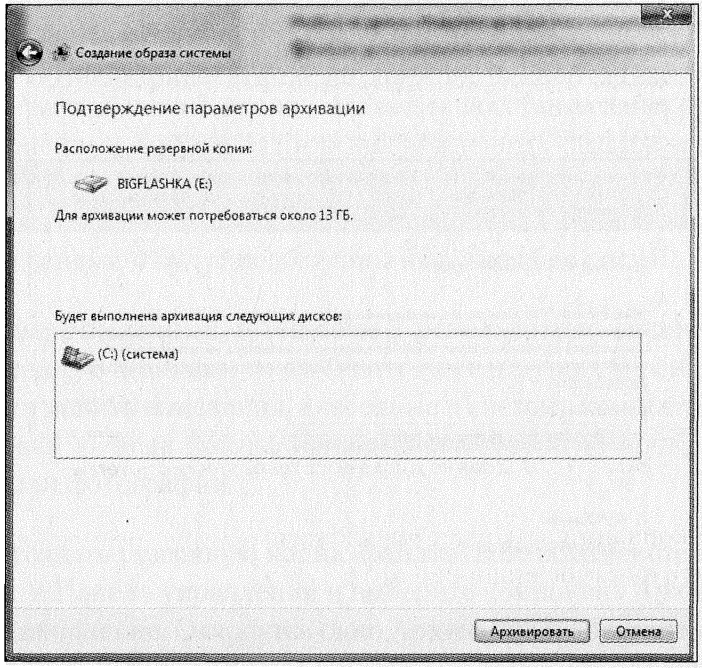


Рис. 8.12. Подтверждение параметров архивации

создать диск восстановления системы. Если у вас его еще нет, то рекомендуется его создать. Дело в том, что созданный образ системы сам по себе ничего не представляет. Это просто папка с набором файлов. Для использования её при восстановлении системы нужен специальный компонент либо диск. Поэтому необходимо создать его. В принципе, диск можно создать и позже из окна резервного копирования (см. рис. 8.10).

Создание диска восстановления системы

Щелкните кнопку **Да**. На экране отобразится диалоговое окно выбора привода компакт-диска, в котором должна быть вставлена пустая болванка. Выберите нужный привод, вставьте в него пустой компакт-диск и щелкните кнопку **Создать диск**. Начнется процесс создания диска (рис. 8.13).

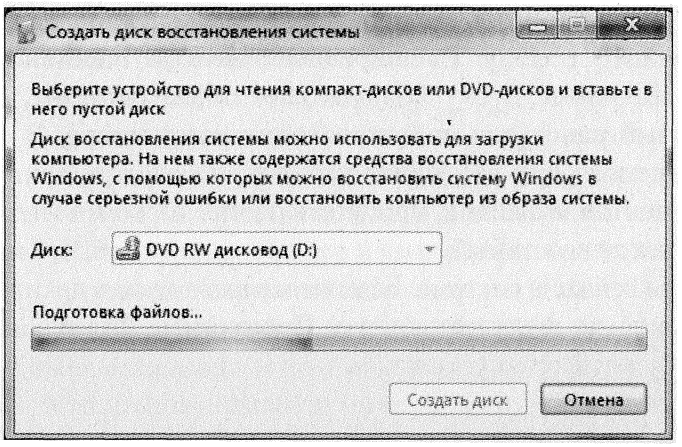


Рис. 8.13. Создание диска восстановления системы

По его окончании вам будет предложено подписать его (правда) и положить на самое видное место (шутка).

Восстановление компьютера по резервной копии образа системы

Данное восстановление производится обычно при серьезных сбоях системы или при полной её неработоспособности. Однако стоит помнить, что восстановление из образа системы приведет к тотальной замене всех системных и пользовательских файлов вашего компьютера. То есть ваш компьютер будет в точности соответствовать системе на день записи образа диска. В связи с этим рекомендуется по возможности чаще снимать образы диска.

Восстановить компьютер по образу системы можно несколькими способами. Ниже мы рассмотрим каждый из них, так как этот вопрос очень важен для каждого пользователя.

1. **Восстановление с помощью компоненты Восстановление.** Данный способ используется в случае, когда еще есть возможность попасть в Панель управления. В панели

управления запустите компонент **Восстановление**. Щелкните ссылку **Расширенные методы восстановления**. Щелкните пункт **Используйте образ системы, созданный ранее для восстановления компьютера**. В открывшемся окне вам будет предложено сделать архив документов и файлов, присутствующих на компьютере. Ведь после восстановления у вас пропадет все то, что находится сейчас в системе. Если не желаете делать архивную копию, то щелкните кнопку **Пропустить**. Далее вам нужно будет перезапустить компьютер и выбрать язык раскладки клавиатуры. Затем вы должны выбрать нужный образ диска (если у вас их несколько). Но при этом вы должны подключить диски, на которые образ системы был сохранен (рис. 8.14).

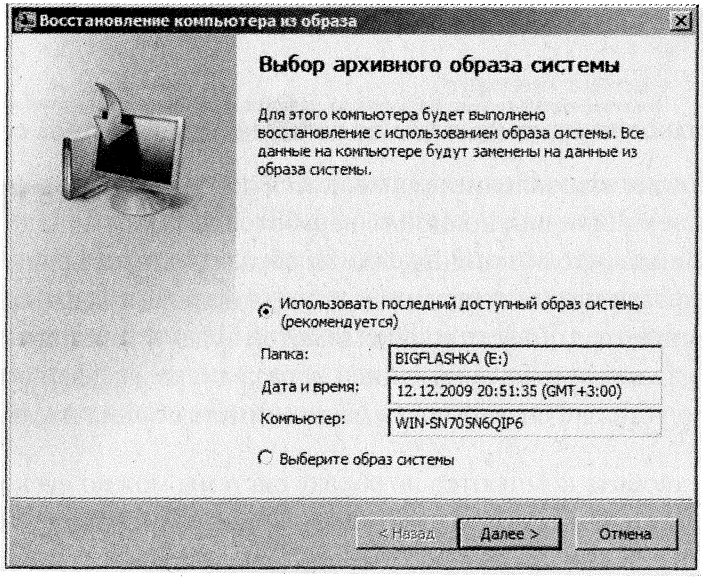


Рис. 8.14. Выбор образа системы

Щелкните кнопку **Далее** и при необходимости сделайте нужные настройки. Для начала процесса останется щелкнуть кнопку **Готово**.

2. **Восстановление с помощью предустановленных параметров восстановления.** Данный способ применяется, когда доступа к Панели управления уже нет, и у вас нет ни установочного диска, ни диска восстановления, а запуск Windows еще возможен. Перезапустите компьютер и до начала загрузки системы успейте нажать клавишу **F8**. Должен отобразиться экран **Дополнительные варианты загрузки** (рис. 8.15).

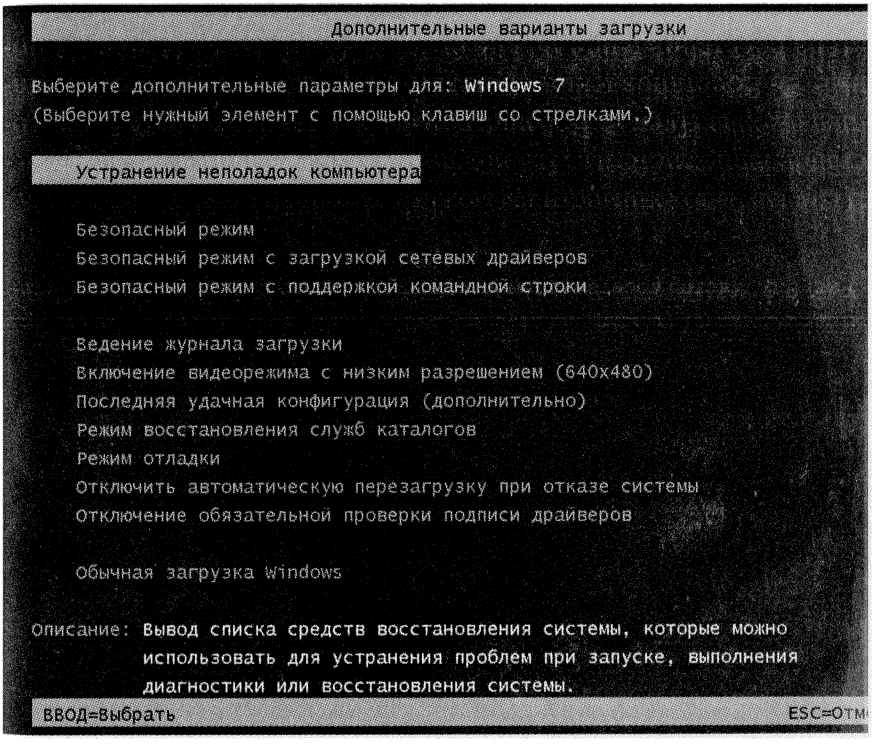


Рис. 8.15. Дополнительные варианты загрузки

Выберите пункт **Устранение неполадок компьютера**. Далее выберите раскладку клавиатуры и нажмите кнопку **Далее.** Выберите имя пользователя, введите пароль и нажмите кнопку **ОК**. В меню **Параметры восстановления**

системы выберите пункт **Восстановление образа системы.** Откроется окно выбора образа (см. рис. 8.14). Дальнейшие действия такие же, как и в предыдущем способе восстановления.

3. **Восстановление с помощью установочного диска Windows или диска восстановления системы.** Вставьте в привод установочный диск или диск восстановления системы и перезагрузите компьютер. При запросе нажмите любую клавишу для запуска компьютера с установочного диска или диска восстановления системы. Выберите параметры языка и нажмите кнопку **Далее**. Выберите **Восстановить компьютер**. В меню **Параметры восстановления системы** выберите пункт **Восстановление образа системы**. Откроется окно выбора образа (см. рис. 8.14). Дальнейшие шаги вы уже знаете.

8.3.2. Резервное копирование файлов

Вместо создания образа всего компьютера вы можете создавать архивы выбранных файлов. Если программа архивации Windows используется впервые, в компоненте **Архивация и Восстановление файлов** щелкните пункт **Настроить резервное копирование**. Произойдет сканирование системы, и откроется окно выбора хранилища архива (рис. 8.16).

Выберите носитель информации, где вы желаете сохранить свой архив, и щелкните кнопку **Далее**. Откроется окно выбора файлов, для которых желаете создать резервную копию (рис. 8.17).

Вы можете предоставить выбор файлов операционной системе. В данном случае в резервную копию войдут файлы данных, сохраненные в библиотеках, на рабочем столе и в папках Windows

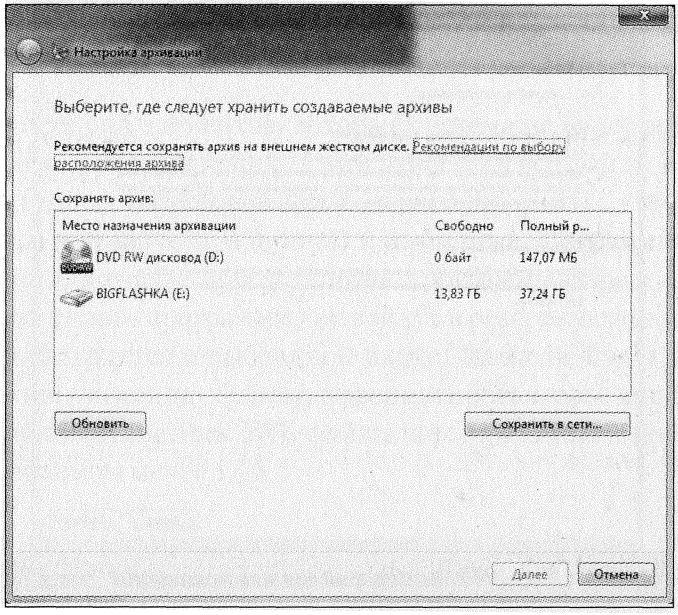


Рис. 8.16. Выбор месторасположения архива

по умолчанию для всех пользователей с учетной записью на этом компьютере. Папками Windows по умолчанию являются: **AppData**, **Контакты**, **Рабочий стол**, **Загрузки**, **Избранное**, **Ссылки**, **Сохраненные игры** и **Поиски**. Следует помнить, что если диск, на котором сохраняется резервная копия, отформатирован с использованием файловой системы NTFS и на нем достаточно места, то архив будет содержать еще и образ системы.

Поэтому, если вам не требуются архивы всех перечисленных папок, то выберите самостоятельно, что хотите сохранить. Для этого включите переключатель **Предоставить мне выбор** и щелкните кнопку **Далее**. Откроется окно выбора файлов (рис. 8.18).

С помощью древовидной структуры отметьте флажками все интересующие вас объекты. Также здесь можно отключить создание

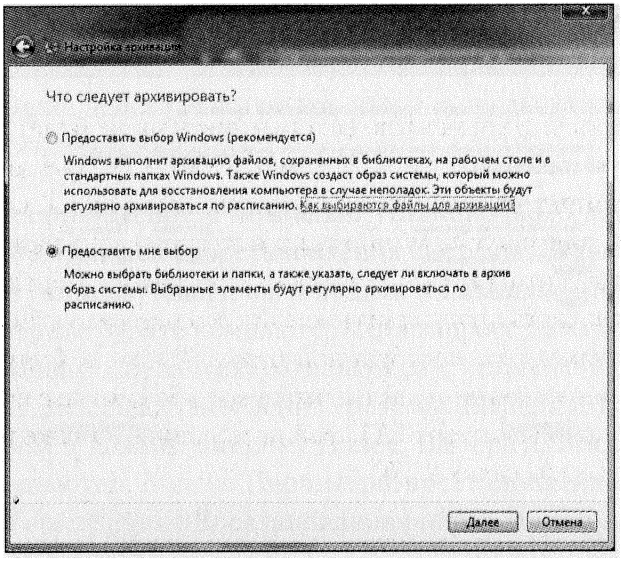


Рис. 8.17. Выбор файлов для архивации

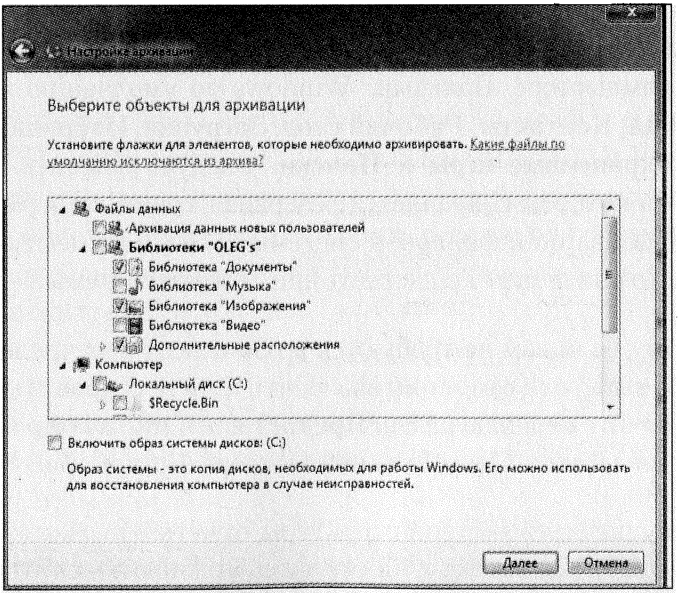


Рис. 8.18. Самостоятельный выбор файлов для архивной копии

образа системы, что существенно сэкономит место ваших хранилищ.

Однако есть ряд элементов, которые система не будет архивировать ни при каких условиях. К ним относятся все файлы в известных системных папках (то есть содержащих файлы, которые необходимы для запуска Windows) и известные программные файлы (файлы, которые при установке программы определяются в реестре как часть программы) не войдут в резервную копию, даже если они находятся в выбранной папке. Также не будут включены в архивную копию файлы, отформатированные с использованием файловой системы FAT, файлы корзины, а также временные файлы объемом менее 1 Гб.

Как только вы определитесь со всеми элементами, щелкните кнопку **Далее**. Откроется окно, в котором будет отображена сводка выбранных элементов для архивации.

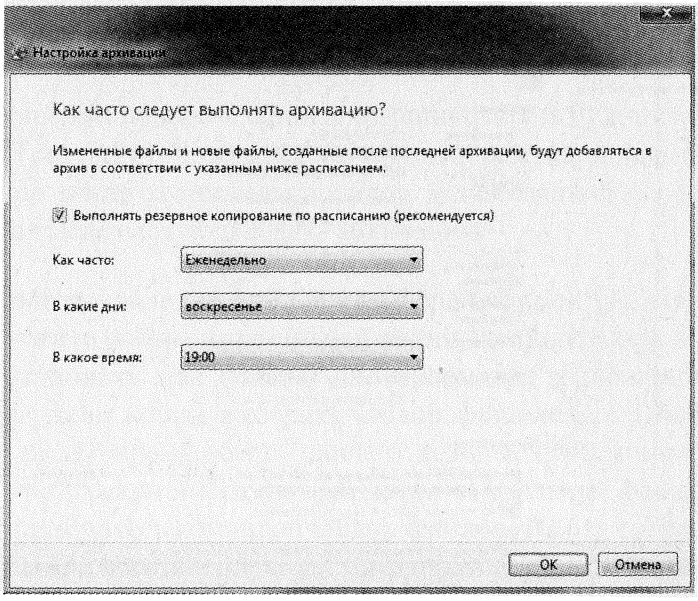


Рис. 8.19. Создание расписания архивации

Ниже показано расписание создания резервных копий. Если оно вас не устраивает, можно изменить его, щелкнув ссылку **Изменить расписание**. В открывшемся окне выберите частоту, день и время создания архива (рис. 8.19).

Здесь же можно совсем отказаться от создания резервной копии по расписанию, убрав флажок. После этого вы сможете архивировать объекты только вручную. Подтвердите изменения с помощью кнопки **ОК**.

И в заключение настройки архивации щелкните кнопку **Сохранить параметры и запустить архивацию**. Немедленно начнется процесс архивации (рис. 8.20).

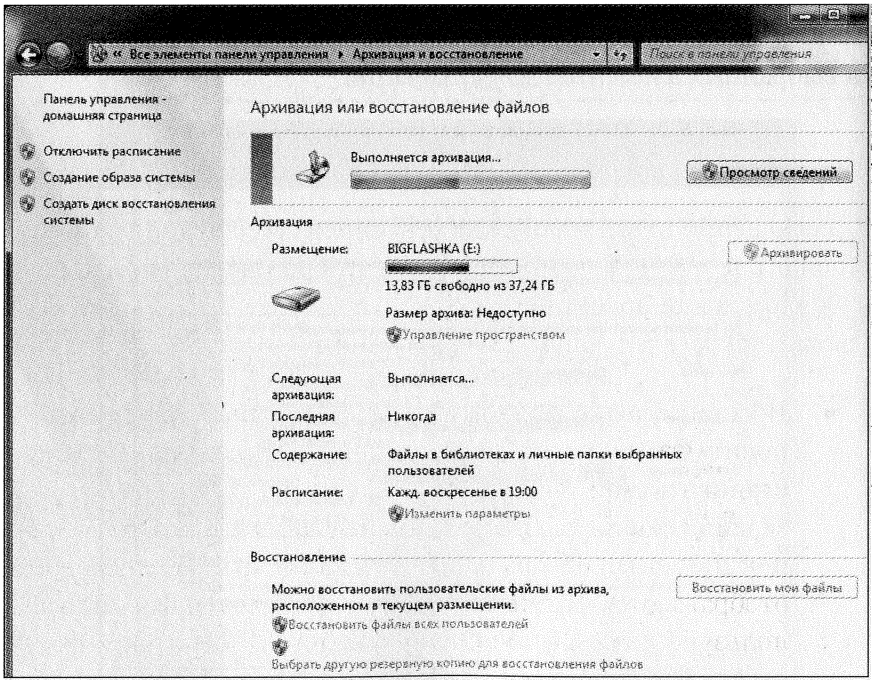


Рис. 8.20. Выполнение архивации

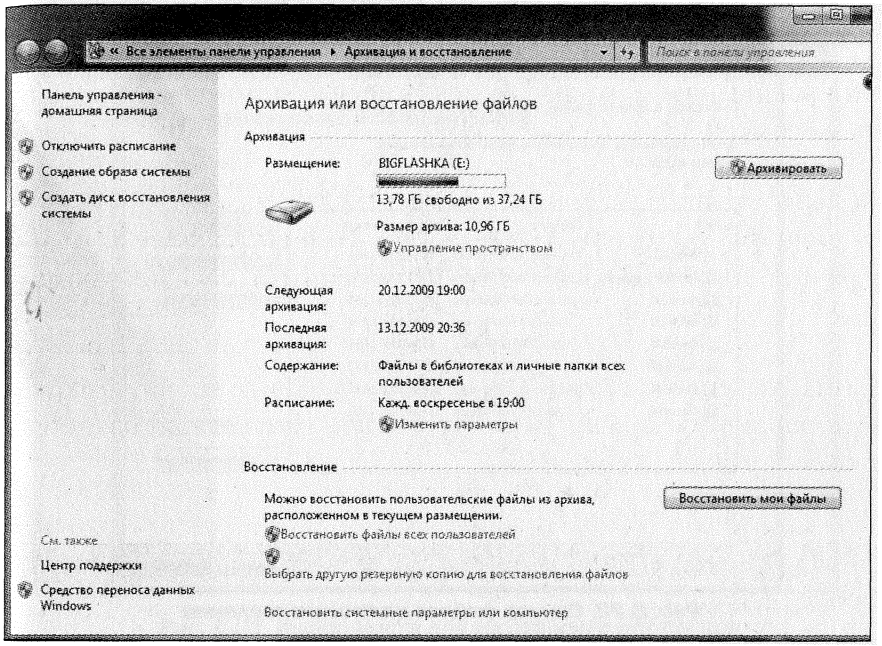


Рис. 8.21. Окно архивации и восстановления файлов

По завершении процесса окно архивации файлов будет иметь такой вид (рис. 8.21). Теперь здесь будет отображена информация о свободном месте хранилища архивов, дата создания последнего архива, а также следующая дата архивации.

- Восстановление файлов из резервной копиЧтобы восстановить файлы из резервной копии, щелкните кнопку **Восстановить мои файлы**. Для просмотра содержимого резервной копии выберите **Обзор файлов** или **Обзор папок**. Во время обзора папок отдельные файлы в папке не отображаются. Чтобы просмотреть отдельные файлы, воспользуйтесь командой **Обзор файлов.** Выберите все файлы для восстановления с помощью кнопки **Добавить** (рис. 8.22).

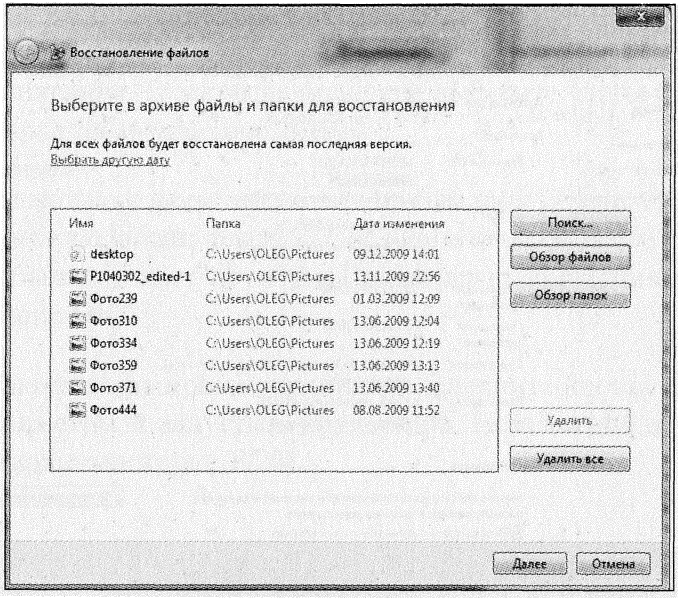


Рис. 8.22. Список файлов для восстановления

- Щелкните кнопку **Далее**. Откроется окно, где вы должны определить место, куда выбранные файлы будут восстановлены (рис. 8.23). Это либо старое их местоположение, либо новое место, определенное вами. Как только вы определитесь с выбором, щелкните кнопку **Восстановить**.

Восстановление файлов из предыдущих версий

На наш взгляд, это очень нужное нововведение Windows 7 сохранит нервы многим пользователям. При невозможности восстановления файлов предыдущими способами попытайтесь реанимировать предыдущую версию файла, так как Windows 7 автоматически сохраняет их. Таким образом, восстанавливаются не только файлы, но и папки.

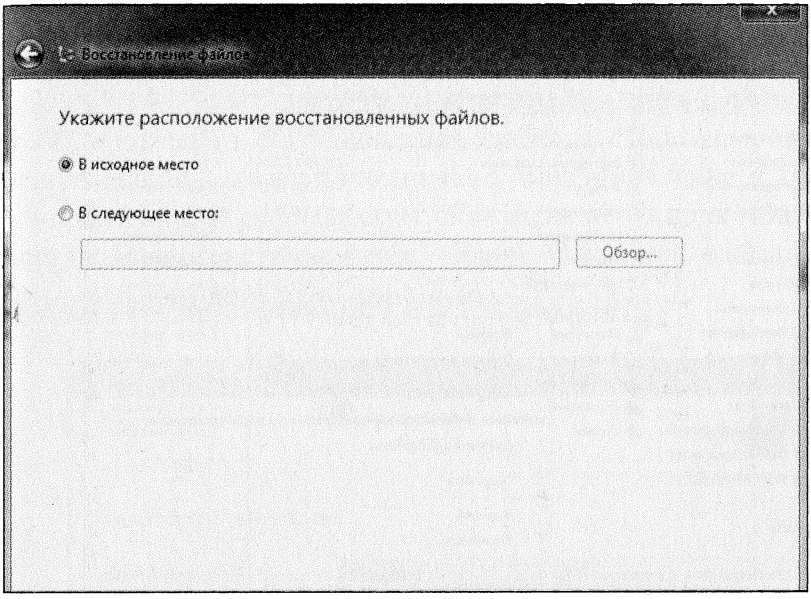


Рис. 8.23. Выбор места для восстановления файлов

Для того чтобы восстановить предыдущую версию, просто найдите папку, где хранился файл, и щелкните её правой кнопкой (рис. 8.24).

В контекстном меню выберите пункт **Восстановить прежнюю версию**. Появится список предыдущих версий файла или папки (рис. 8.25).

Выберите нужную версию и щелкните кнопку **Открыть**, чтобы убедиться, что это именно та версия, которая нужна. Чтобы восстановить предыдущую версию, выберите ее и нажмите кнопку **Восстановить.**

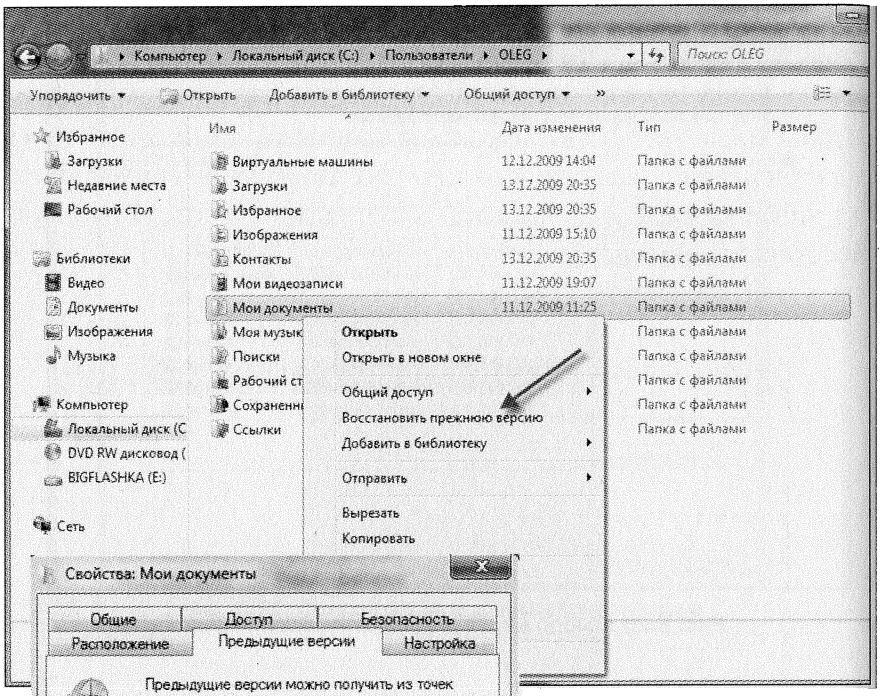


Рис. 8.24. Восстановление предыдущих версий файлов

Рис. 8.25. Список предыдущих версий файла или папки

8.3.3. Восстановление компьютера до предыдущего рабочего состояния

Чтобы произвести восстановление системы с помощью точек восстановления, запустите компонент **Восстановление** в Панели управления. В открывшемся окне щелкните кнопку **Запуск восстановления системы**. Затем – **Далее**. Откроется окно со списком точек восстановления (рис. 8.26).

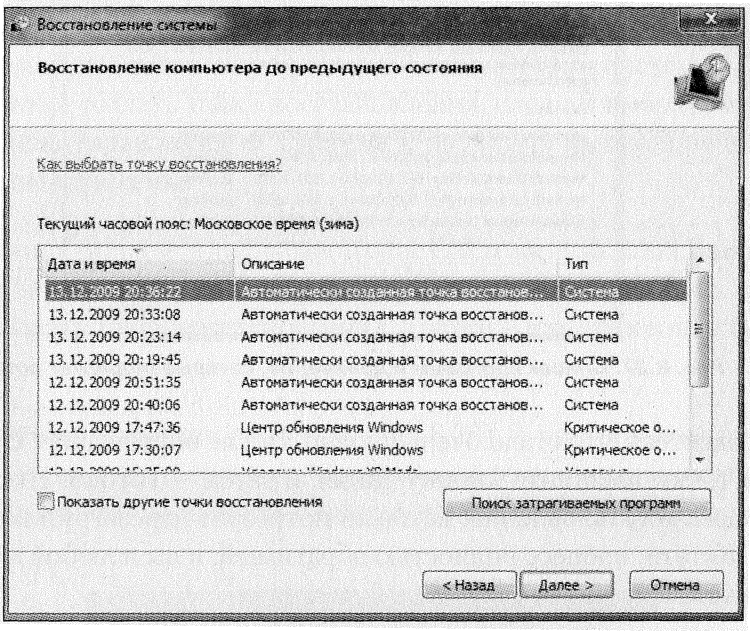


Рис. 8.26. Список точек восстановления

Выберите нужную точку. Интересным нововведением в Windows 7 стала опция поиска затрагиваемых программ. Смысл её в том, что вы сможете просмотреть список всех программ, которые будут удалены при выборе определенной точки, а также список тех, которые будут восстановлены. Для этого просто щелкните кнопку Поиск затрагиваемых программ. Откроется список программ и драйверов (рис. 8.27).

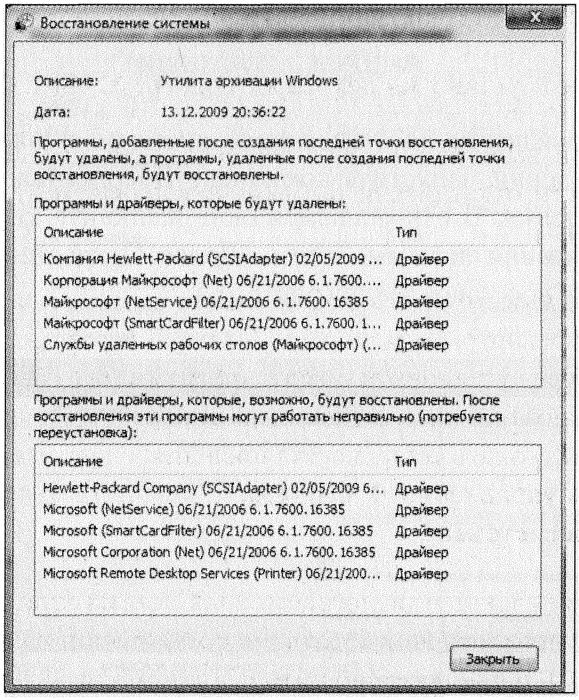


Рис. 8.27. Список программ и драйверов, которые подлежат ротации

Согласитесь, что стало очень удобно. После определения с выбором точки щелкните кнопку **Далее** и затем – **Готово**. Начнется процесс восстановления, который потребует перезагрузки системы. Кстати, процесс полностью обратимый, и вы в любой момент сможете изменить точку на любую другую.

Точки восстановления обычно автоматически создаются в следующих ситуациях:

- При первом запуске компьютера после установки и обновления.
- При установке новых драйверов.

- В соответствии с принятым расписанием.
- После установки некоторого программного обеспечения.
- При выполнении восстановления системы (для возможности отката, если выбрана неудачная контрольная точка).

Однако вы можете сами в любой момент создать точку восстановления, чтобы потом можно было бы к ней вернуться. Это бывает полезно перед установкой нового программного обеспечения или перед масштабными изменениями в параметрах системы. Для того чтобы создать точку восстановления, следует выбрать **Пуск ➔ Панель управления ➔ Система** и щелкнуть мышкой по задаче **Защита системы**.

Далее в появившемся диалоговом окне **Система** на вкладке **Защита** вам будет предложено выбрать диск или диски, на которых следует создать точки восстановления, а затем – нажать кнопку **Создать**.

После этого появится окно (см. рис. 8.28), в котором вам будет предложено ввести описание создаваемой точки восстановления. Можете ничего не вводить. Однако, чтобы потом не запутаться,

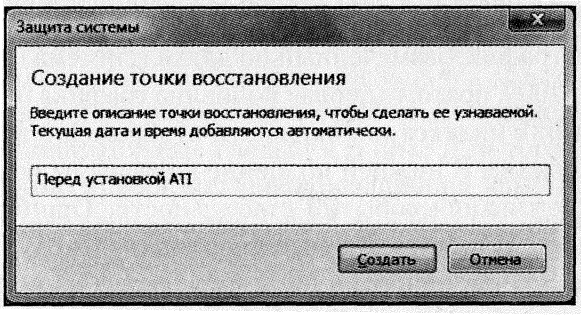


Рис. 8.28. Ввод названия контрольной точки

для себя рекомендуется указать, что это за точка. Нажмите **Создать** — и точка восстановления будет создана. Закрывать все приложения при этом не обязательно. Перезагрузка компьютера производиться не будет.

8.3.4. Монитор стабильности системы

Монитор стабильности системы является внешней оснасткой Windows, отображающей в хронологическом порядке индекс стабильности системы. Значение индекса зависимо от любого изменения, внесенного в конфигурацию компьютера, или возникшей проблемы компьютера. Кроме того, с помощью монитора можно ознакомиться с подробными сведениями о событии, которое каким-то образом повлияло на стабильность системы, в определенный день. В свою очередь, все события системы хранятся один год.

Чтобы ознакомиться с индексом стабильности системы, в панели инструментов перейдите в компонент **Центр поддержки**. Щелкните **Обслуживание**, затем – **Показать журнал стабильности работы**. На экране отобразится окно **Монитор стабильности системы** (рис. 8.29).

Диаграмма стабильности системы представляет собой прокручивающийся график, размеченный по датам (система была установлена 09.12.2009, поэтому первая половина графика на рисунке пустая). График индекса стабильности отображен в верхней половине диаграммы. В нижней половине диаграммы находятся пять строк отслеживания событий стабильности: **Ошибки приложения**, **Ошибки Windows**, **Разные неполадки, Предупреждения** и **Сведения**. Значки напротив даты означают обнаружение одного из событий стабильности. При успешном завершении установки

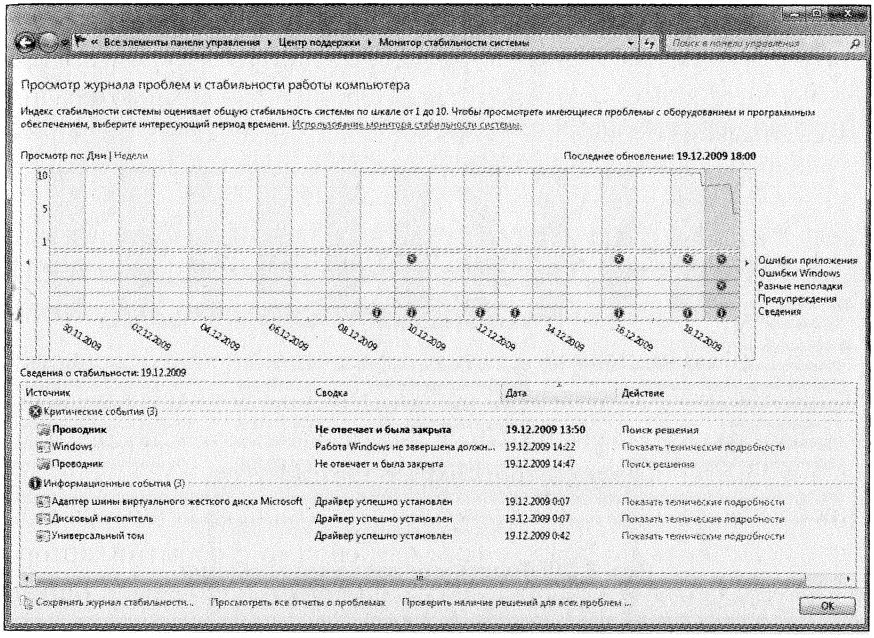


Рис. 8.29. Монитор стабильности системы

или удаления программы появляется значок информации, а при возникновении ошибки в ходе одного из этих процессов появляется значок предупреждения. Если нужная дата находится вне видимости, воспользуйтесь полосой прокрутки в нижней части диаграммы. Для просмотра дополнительных сведений о событии на определенную дату, просто щелкните его на графике (рис. 8.30).

Щелкните любой из элементов в столбце **Действие**, чтобы просмотреть дополнительные сведения о них. Для того чтобы просмотреть только проблемы, произошедшие на компьютере, щелкните **Просмотр всех отчетов о проблемах** внизу окна (рис. 8.31).

Для поиска решения появившейся конкретной проблемы щелкните **Поиск решения**. Незамедлительно начнется поиск и ото-

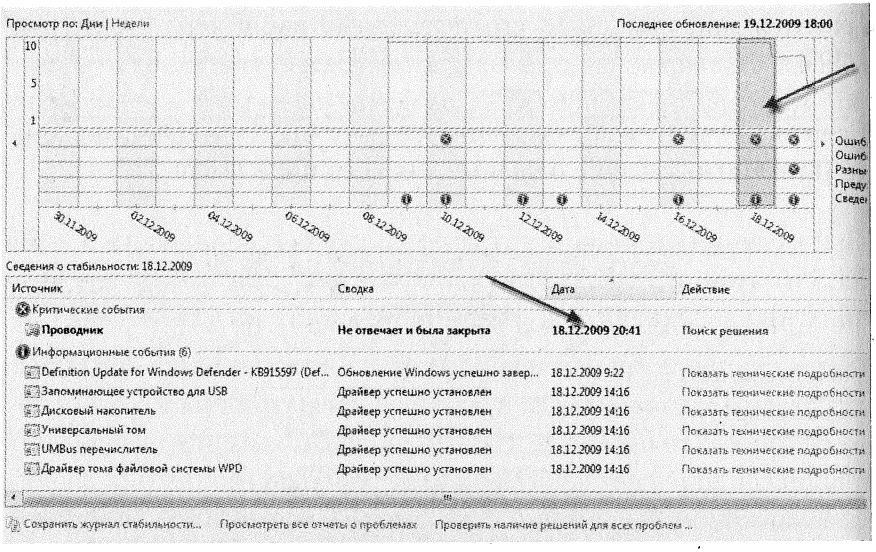


Рис. 8.30. Подробные сведения о событии

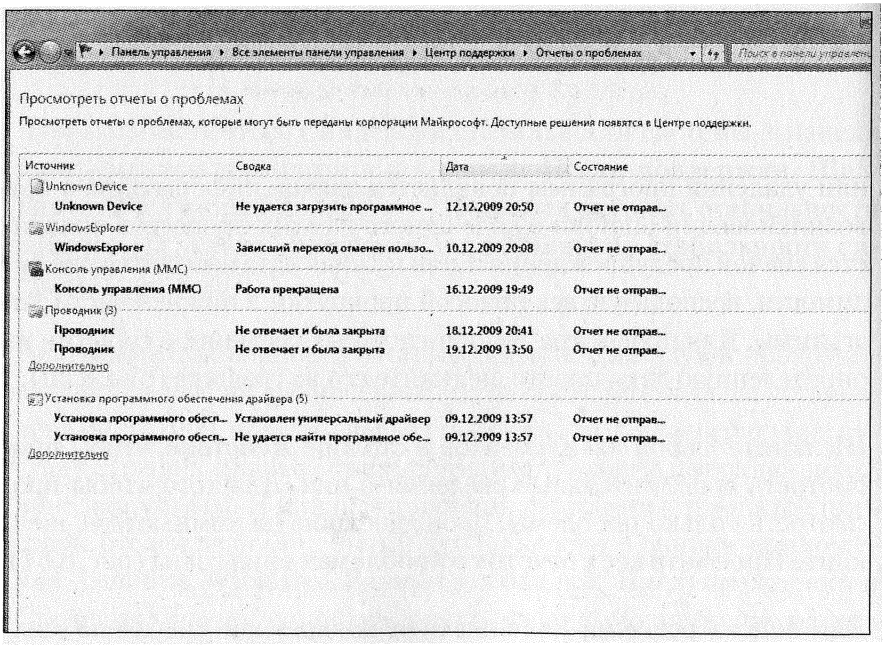


Рис. 8.31. Просмотр отчетов о проблемах

бразится информация о его результате, например, такая (рис. 8.32).

Если вы желаете искать решение для всех проблем сразу, щелкните **Проверить наличие решений для всех проблем** внизу окна.

При желании вы можете сохранить журнал стабильности в файл XLS и затем отправить его куда пожелаете. Для этого щелкните внизу окна **Сохранить журнал стабильности** и введите имя файла.

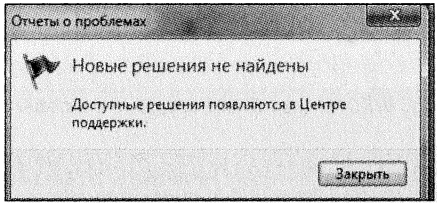
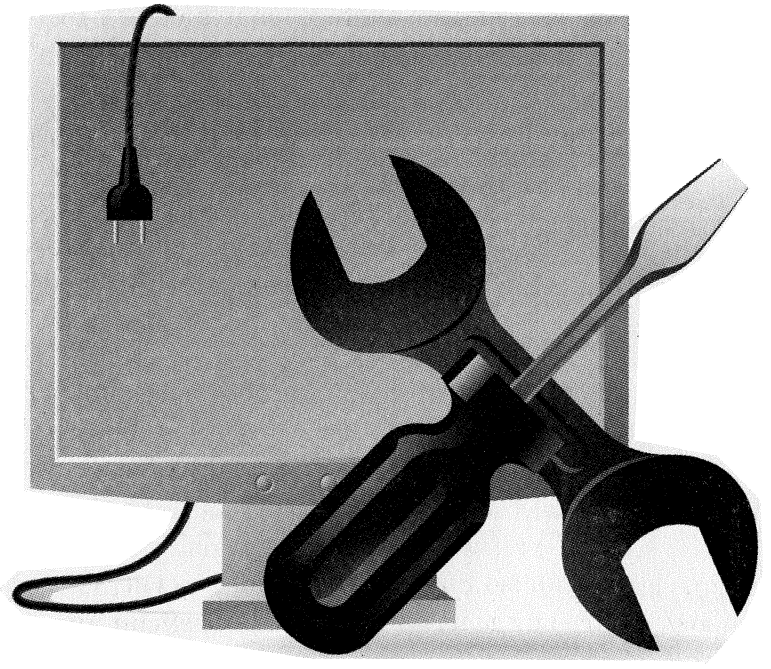


Рис. 8.32. Результат поиска решения

ГЛАВА 9.

ПРИ ЗАГРУЗКЕ КОМПЬЮТЕРА ПОЯВЛЯЕТСЯ СИНИЙ ЭКРАН, И ЗАГРУЗКА ПРЕРЫВАЕТСЯ



9.1. Стоп-ошибки Windows, или о «Синих экранах смерти»

Наверняка у каждого из вас во время работы на компьютере с любой без исключения версии Windows хоть раз возникала ситуация, когда внезапно все текущие задачи прекращались и перед глазами возникал синий экран с белым англоязычным текстом, в котором присутствовала непонятная смесь букв и цифр. Иногда данный экран появлялся лишь однажды, а в других случаях его приходилось наблюдать с нежелательной периодичностью. То, о чем мы сейчас поведем речь, официально называется стоп-ошибкой Windows (Stop error). В народе данную ситуацию прозвали «Синим экраном смерти» или BSOD (от англ. **B**LUE **S**CREEN **O**F **D**EATH). Существует два вида сообщений BSOD: для семейства Microsoft Windows 95/98/Me и для семейства Microsoft Windows NT/2000/XP/2003/Vista/7/8. Здесь мы будем вести разговор о фатальных ошибках, возникающих в операционной системе Windows 7 и иногда 8.

В Windows 7 синий экран смерти появляется при возникновении фатальной ошибки в коде ядра процессора либо его драйвера. Например, если драйвер попытается выполнить операцию, которая не допустима для процессора, результатом станет окраска экрана в синий цвет. Единственным допустимым действием для вас останется выключение компьютера. Хотя этого можно и не делать, так как по прошествии определенного системой времени это произойдет автоматически. В любом случае, все ваши несохраненные данные будут безвозвратно потеряны.

В отличие от XP, в Windows 7 процесс создания отчета о возникшей ошибке (Windows Error Reporting) был модернизирован в сторону автоматизации. Сегодня пользователи Windows 7 вместо синего экрана смерти все чаще могут встретить сообщение следующего содержания: **«Microsoft Windows операционная система не отвечает»**, а пользователю предоставлены для выбора два решения: **Закрыть программу и Ожидание отклика программы** (рис. 9.1).

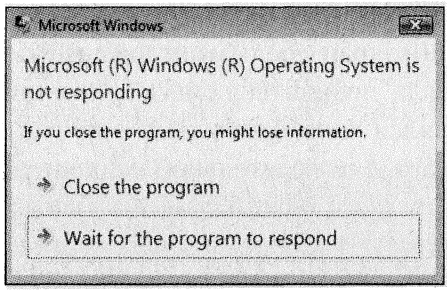


Рис. 9.1. Сообщение, предотвращающее синий экран смерти в Windows 7

Вам предстоит выбрать, либо сразу потерять все незаписанные данные, либо обрести надежду и ждать отклика программы, которого вы, скорее всего, не дождетесь. Хотя... Но давайте вернемся к более экстремальной ситуации когда, все-таки BSOD появился. Разберем, что же там написано.

Текст на синем экране меняется в зависимости от возникшей ситуации, но его формат строго стандартизирован и состоит из трех частей (рис. 9.2):

- в **Части 1** отображается символьное имя ошибки, которое дает операционная система и которое соответствует номеру произошедшей стоп-ошибки;

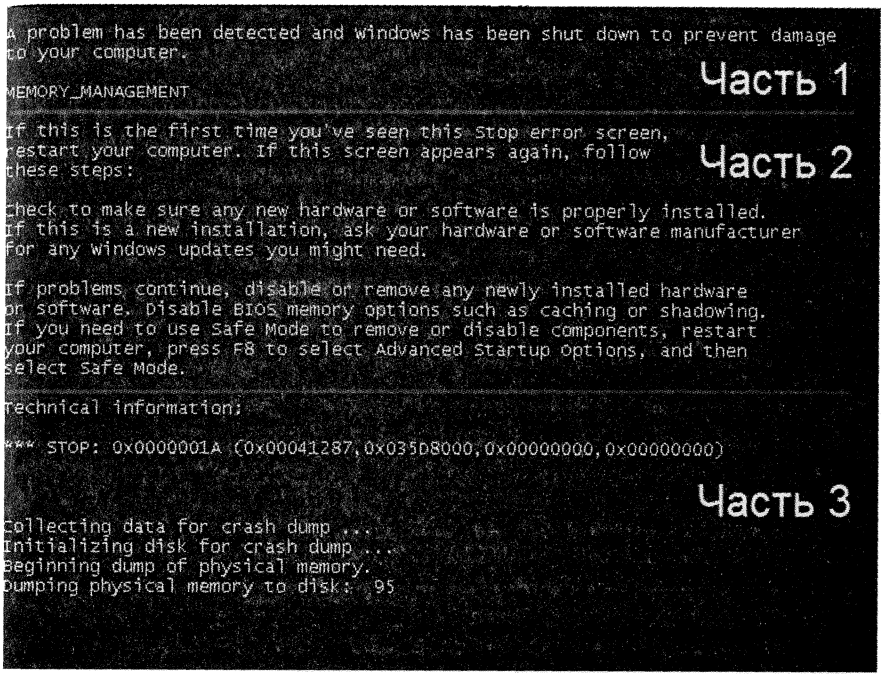


Рис. 9.2. Синий экран смерти в Windows

- в **Части 2** даются рекомендации по разрешению проблемы. Они одинаковы для стоп-ошибок одинакового типа;
- в **Части 3** отображены номер ошибки и её параметры, в которые заключено разъяснение возникшей проблемы и которые предназначены для отладочного ПО. Номер ошибки следует сразу же за словом STOP в шестнадцатеричной системе исчисления. В скобках перечислены 4 параметра ошибки.

Как правило, пользователю практически не предоставлено возможностей для исправления ошибки. Все ограничивается банальной перезагрузкой компьютера в надежде на то, что синий экран смерти произошел в результате несоответствия некоторых драйверов, которое не было выявлено при тестировании. Но даже если

и перезагрузка системы не помогает избавиться от пресловутого синего экрана, то можно попробовать выполнить определенные инструкции. Данные инструкции, так или иначе помогающие решению проблем, вы можете найти на сайте Microsoft либо на других, специализирующихся на тематике разрешения проблем, возникающих при работе с Windows 7. Просто введите символьное имя ошибки либо её имя в поисковой строке, например Google либо другого портала, и вы получите множество ссылок на инструкции по её исправлению. Однако, если быть до конца честными, то вы не найдете ответы на абсолютно любые стоп-ошибки. Но не стоит отчаиваться, так как самые распространенные проблемы давно уже разрешены. Ниже мы опубликуем список самых распространенных стоп-ошибок, встречающихся в Windows 7.

Как мы уже говорили ранее, очень частой причиной синих экранов смерти являются вновь установленные драйверы, либо драйверы, поврежденные в результате различных сбоев компьютера или других внештатных ситуаций, например внепланового прекращения подачи электропитания. Поэтому вы самостоятельно сможете попытаться решить проблему BSOD, если выявите конфликтный драйвер. Вам останется заменить его на более свежий либо, наоборот, вернуться к предыдущему, при котором сбоев не наблюдалось. Если и это не поможет, то можно будет попробовать переустановить программу, установившую драйвер. Вроде бы все понятно, прочитал на синем экране название драйвера, и в путь. Однако не все так просто.

Не все стоп-ошибки отображают имя драйвера. Но, к счастью, имеются альтернативные возможности для определения конфликтного драйвера. Для этого служит дамп памяти (**memory.dmp**). Но сначала нужно удостовериться о том, что ваша система имеет к нему доступ.

9.2. Настройка дампа памяти

Необходимым условием для работы с дампом памяти является наличие файла подкачки на системном диске. Поэтому проверьте на своем компьютере, имеет ли раздел диска, на который установлена Windows, файл подкачки. Для этого щелкните правой кнопкой **Компьютер→Свойства**. В открывшемся окне **Система** щелкните **Дополнительные параметры системы**. Откроется окно **Свойства системы**. Перейдите во вкладку **Дополнительно**. В разделе **Быстродействие** щелкните кнопку **Параметры**. В открывшемся окне **Параметры быстродействия** перейдите во вкладку **Дополнительно** и щелкните кнопку **Изменить.** Откроется окно **Виртуальная память** (рис. 9.3).

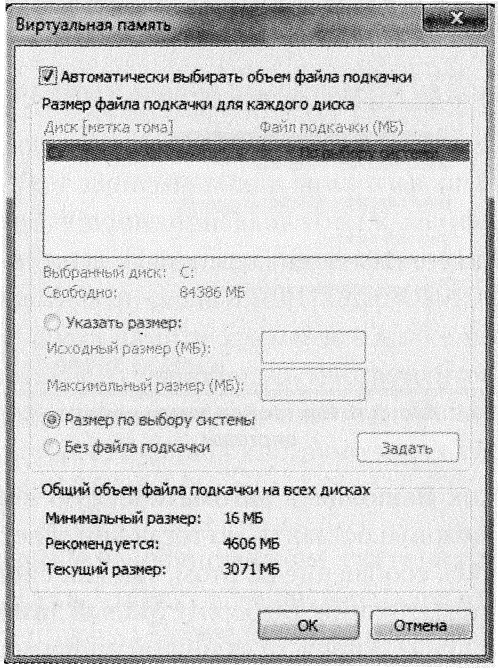


Рис. 9.3. Редактирование файла подкачки

В данном окне вы можете управлять размером виртуальной памяти, но это отдельная тема, а для того, чтобы существовал дамп памяти, достаточно и автоматического выбора объема файла подкачки (см. рис. 9.3). Самое главное — не активировать пункт **Без файла подкачки**. Далее вернитесь в окно **Свойства системы.** В разделе **Загрузка и восстановление** щелкните кнопку **Параметры**. Откроется окно **Загрузка и восстановление** (рис. 9.4).

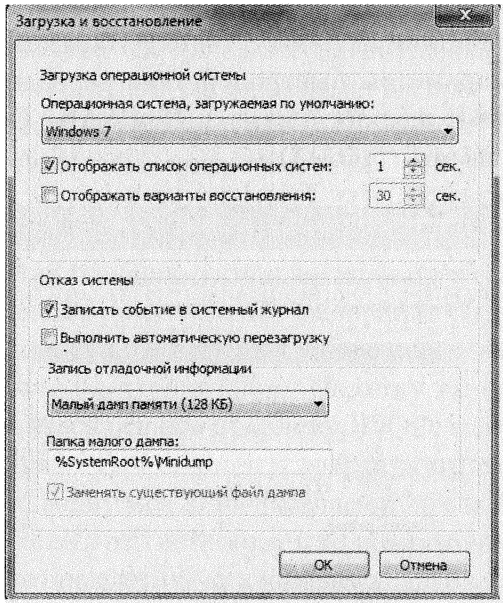


Рис. 9.4. Настройка дампа памяти системы

Снимите флажок **Выполнить автоматическую перезагрузку**. В принципе, его можно и оставить, но тогда при сбое системы вы не успеете прочитать сообщение об этом, так как система будет перезагружена автоматически. Выберите **Малый дамп памяти** в раскрывающемся списке **Запись отладочной информации**.

По умолчанию папка для будущих дампов будет находиться в системном каталоге. Вы можете изменить её местоположение в

поле **Папка малого дампа**. Но делать это рекомендуется лишь в самых исключительных случаях. Щелкните кнопку **ОК**, чтобы записать настройки. Теперь все готово для записи ваших критических ошибок. Если кто-то пытается найти папку **c:\Windows\minidump**, то вы не найдете её. Вернее, не найдете до первого появления синего экрана смерти. Если BSODa не было, то и папки не будет. Далее мы будем рассматривать случаи возникновения стоп-ошибок.

9.3. Выуживаем информацию из дампа памяти с помощью программы Debugging Tools for Windows

Настройка программы и анализ дампа памяти из консоли

Итак, теперь вся подробная информация при возникновении стоп-ошибки будет записываться в дамп памяти. Но как же воспользоваться ею? Windows присваивает каждому файлу отдельное имя с указанием даты. Например, Mini040610-01.dmp — это первый файл дампа памяти, созданный 6 апреля 2010 г. Список всех файлов малого дампа памяти хранится в папке %SystemRoot%\Minidump. Существует множество инструментов для их чтения. Самым, пожалуй, доступным является **Debugging Tools for Windows**. К тому же это родной инструмент для Windows, так как создан под крышей Microsoft.

Скачать его можно на официальном сайте поддержки Microsoft, а точнее здесь: http://www.microsoft.com/whdc/Devtools/Debugging/default.mspx. **Debugging Tools for Windows** поддерживает Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows Server 2008 R2 и Windows 7. Кроме того, есть 32- и 64-битная версия ути-

литы. Владельцам 32-битных платформ нужно щелкнуть ссылку **Install Debugging Tools for Windows 32-bit Version**.

В отличие от предыдущих версий, где утилита являлась самостоятельным приложением, начиная с релиза **6.12.x.x** она входит в состав пакета **Windows Driver Kit (WDK).** Поэтому, если вы хотите иметь самую последнюю версию, потребуется скачать весь пакет (620 Мб), а затем вручную установить **Debugging Tools for Windows.** Если вам не нужна новая версия, то выберите любую из предоставленного внизу списка. Для установки самого последнего релиза выполните следующее:

1. Скачайте WDK по ссылке http://www.microsoft.com/whdc/DevTools/WDK/WDKpkg.mspx.

2. Файл будет иметь формат ISO, поэтому откройте его любой программой, работающей с файлами-образами.

3. Откройте на виртуальном диске папку **Debuggers** и запустите файл установщика приложения, соответствующий вашей системе. В нашем случае это **setup_x86**. Следуйте указаниям мастера установки.

4. После завершения установки **Debugging Tools for Windows** загрузите на свой компьютер файл сценария **kdfe.cmd**. Его легко найти с помощью любой поисковой системы.

5. Если Debugging Tools for Windows был установлен не в стандартную папку, то необходимо будет внести изменения в переменную **dbgpath** файла kdfe.cmd. С помощью текстового редактора, например notepad, откройте файл сценария и укажите для переменной **dbgpath** путь к утилите (рис. 9.5).

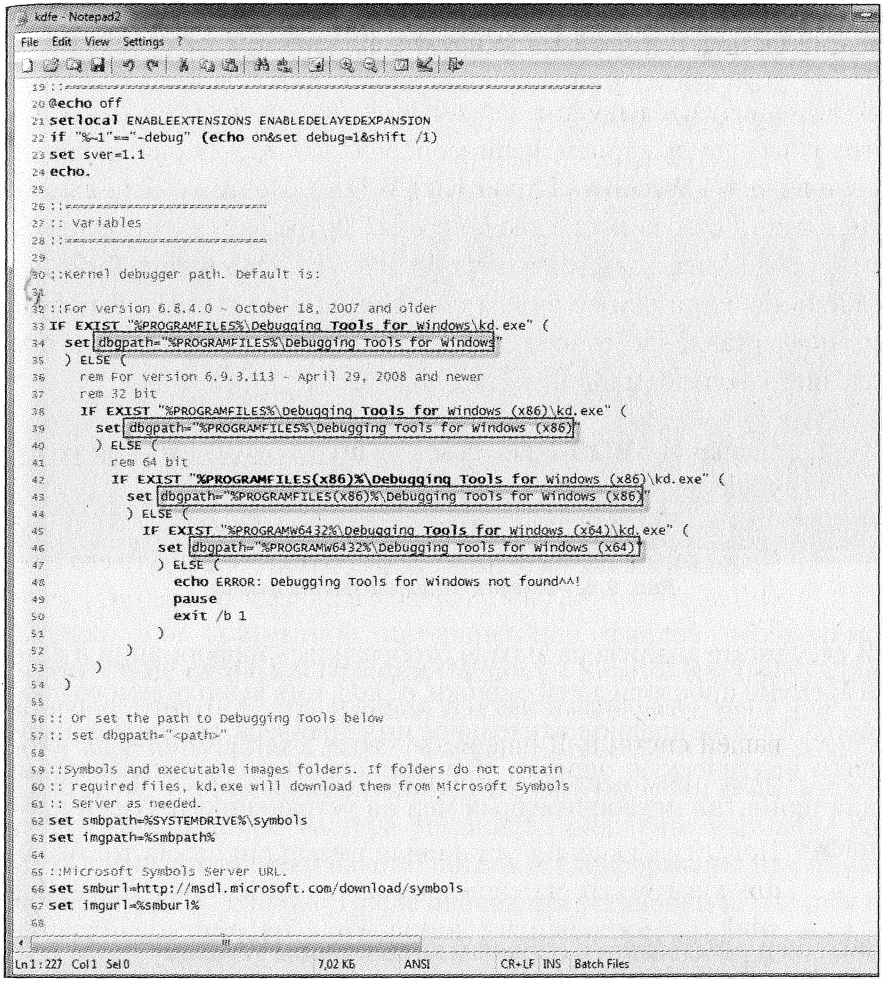


Рис. 9.5. Изменение пользовательского пути к Debugging Tools for Windows

6. Запустите файл kdfe.cmd. Откроется системная консоль Windows, в которой будут перечислены образовавшиеся файлы дампов (**Following crash dump files found**). Их должно быть столько, сколько синих экранов вы «пережили». Следующий вопрос (**Which one would you like to an-**

alyze?) предлагает вам указать порядковый номер файла дампа, который вы желаете анализировать. Введите нужный номер и нажмите клавишу **Enter**. Анализ файла займет некоторое время, после которого на экране отобразится его результат (рис. 9.6).

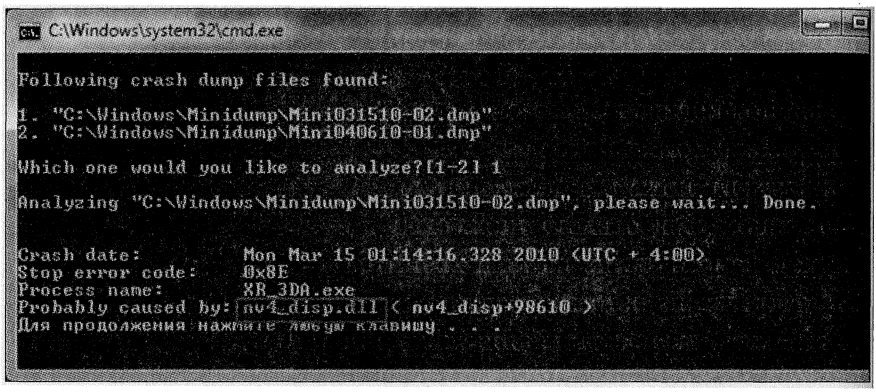


Рис. 9.6. Результат анализа файла дампа

В результате анализа на экране отобразилась информация о дате и времени произошедшей ошибки, её код, имя выполняемого процесса, а также предположительное имя драйвера, спровоцировавшего критическую ошибку. Что нам, собственно, и необходимо для принятия первоочередных мер по устранению текущей проблемы.

Анализ дампа памяти с оконным интерфейсом WinDbg

В рассмотренном примере мы провели анализ файла дампа памяти с помощью консоли. Но в пакете Debugging Tools for Windows имеется инструмент для анализа файлов с аварийными дампами с оконным интерфейсом. Называется он **WinDbg**. Для его запуска щелкните кнопку **Пуск→Все программы→ Debugging Tools for Windows→WinDbg.** Откроется главное окно утилиты (рис. 9.7).

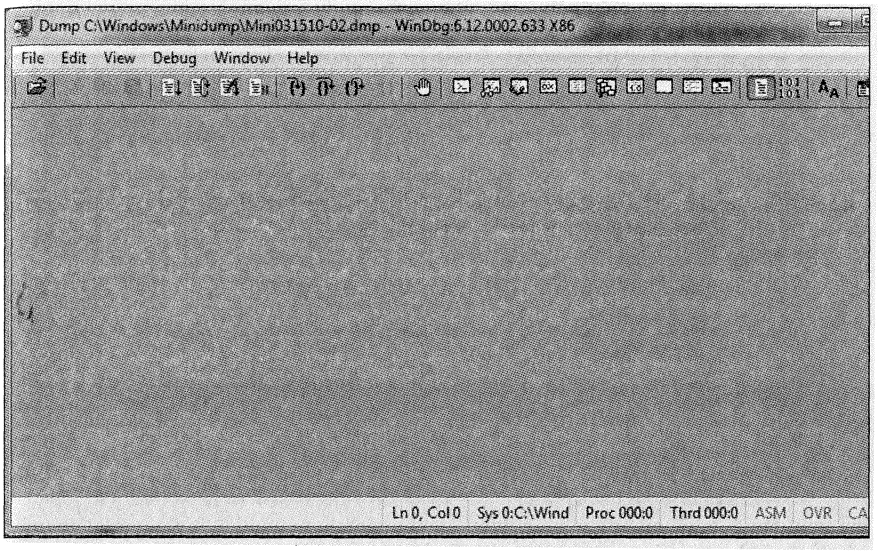


Рис. 9.7. Утилита для анализа файлов дампов памяти

Однако для корректной интерпретации файлов необходимо иметь пакет символов отладки (Windows Symbol Rackeges). Для этого перейдите по следующей ссылке и выберите пакет для вашей версии Windows: http://www.microsoft.com/whdc/devtools/debugging/symbolpkg.mspx. Запустите загруженный файл и следуйте инструкциям мастера установки. Обратите внимание на путь к папке установки пакета, так как эта информация нам понадобится в дальнейшем. После окончания установки перейдите в окно утилиты **WinDbg.** Щелкните меню **File→Symbol File Path...** В открывшемся диалоговом окне **Symbol Search Path** укажите путь к папке **Symbols** (вот зачем нам нужно было его запомнить). Для этого щелкните кнопку **Browse** и выберите путь. Щелкните **ОК** (рис. 9.8).

Вот теперь все готово для выполнения анализа файлов дампа памяти. Щелкните меню **File→ Open Crash Dump.** В открывшемся диалоговом окне выберите уже знакомый нам файл дампа памя-

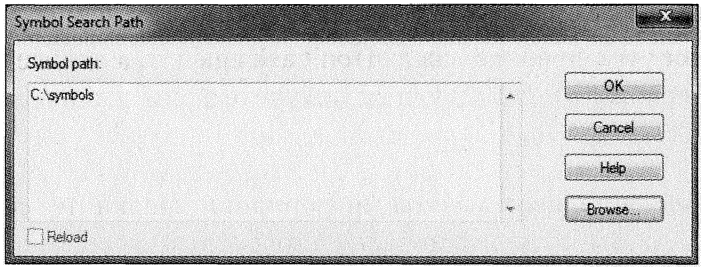


Рис. 9.8. Путь к пакету символов

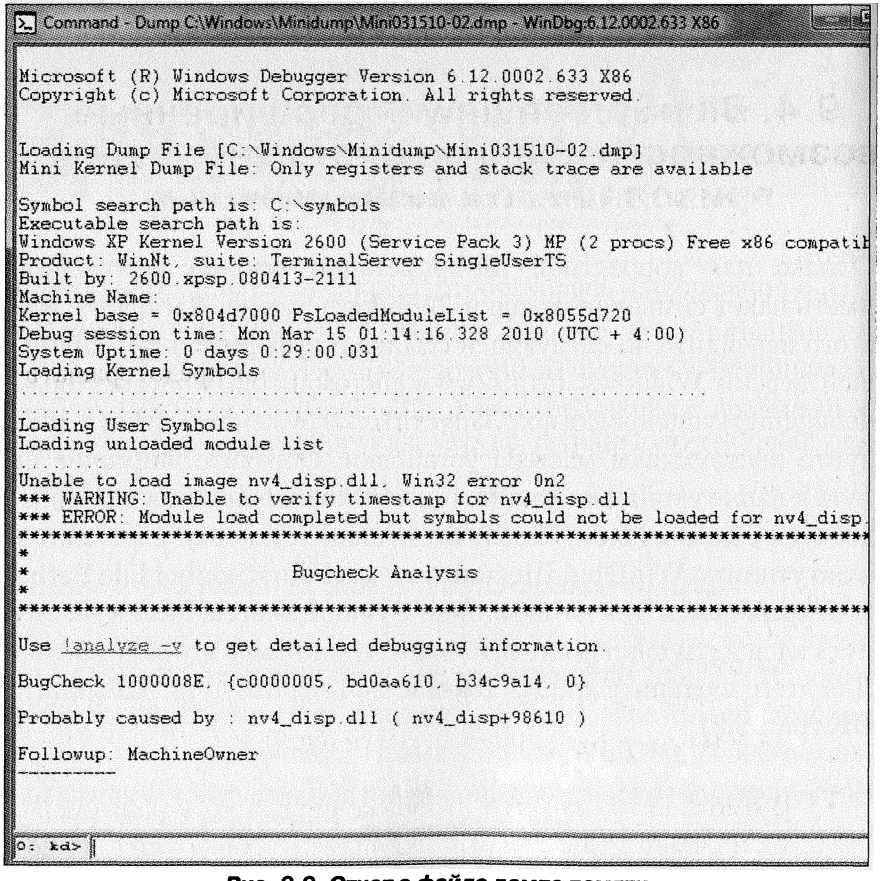


Рис. 9.9. Отчет о файле дампа памяти

ти и щелкните кнопку **Открыть**. На вопрос **Save information for workspace**? установите флажок **Don't ask again** и щелкните кнопку **No**. Через несколько секунд вы получите окно с анализом файла (рис. 9.9).

Для более детализированной информации щелкните ссылку **!analyze –v**. Вы получите довольно подробный отчет о произошедшей ошибке системы. А теперь перейдем к рассмотрению другой, довольно распространенной утилите чтения дампов памяти.

9.4. BlueScreenView — расширенные возможности анализа системного сбоя, приводящего к синему экрану

Утилита, разработанная компанией Nirsoft, также предназначена для подробного изучения мини-дампов, но, в отличие от выше рассмотренного инструмента, имеет несколько дополнительных возможностей, которые помогают пользователю предотвращать появление синих экранов смерти. BlueScreenView сканирует все файлы папки **Minidump**, созданные во время возникновения синего экрана смерти, и отображает информацию обо всех критических стоп-ошибках в одной таблице.

Основные функции BlueScreenView:

- Автоматическое сканирование папки Minidump и отображение списка всех аварийных дампов, включая дату и время, а также детали произошедшей ошибки.

- Возможность «живого» отображения синего экрана смерти, подобно тому, который появился на вашем дисплее во время сбоя. Данная возможность очень помогает в тех слу-

чаях, когда вы не успеваете внимательно изучить BSOD, например, при включенной опции **Выполнить автоматическую перезагрузку,** рассмотренной выше.

- Перечисляет адреса памяти внутри аварийного стека, а также обнаруживает все драйвера и модули, так или иначе причастные к произошедшему сбою.

- Позволяет работать с другими операционными системами Windows, установленными на компьютере с помощью простого изменения пути к папке Minidump нужной ОС.

- Автоматический поиск драйверов, присутствующих в сбойном дампе, и извлечение из них различной информации, такой как название приложения, версии файла, название компании-производителя, а также описание файла.

Скачать утилиту (121 Кб) можно на сайте производителя http://www.nirsoft.net/utils/bluescreenview_setup.exe. Там же можно скачать файл локализации на русский язык http://www.nirsoft.net/utils/trans/bluescreenview_russian.zip. Запустите установочный файл утилиты и следуйте подсказкам мастера. Затем распакуйте файл локализации и поместите его в папку утилиты. По умолчанию это **C:\Program Files\NirSoft\BlueScreenView** . Запустите утилиту. Откроется окно приложения BlueScreenView, разделенное по горизонтали на две части (рис. 9.10).

В верхней части отображается список файлов дампов. По каждому файлу предоставлена следующая информация:

- **Файл дампа:** имя файла дампа памяти, в котором хранятся данные об ошибке.

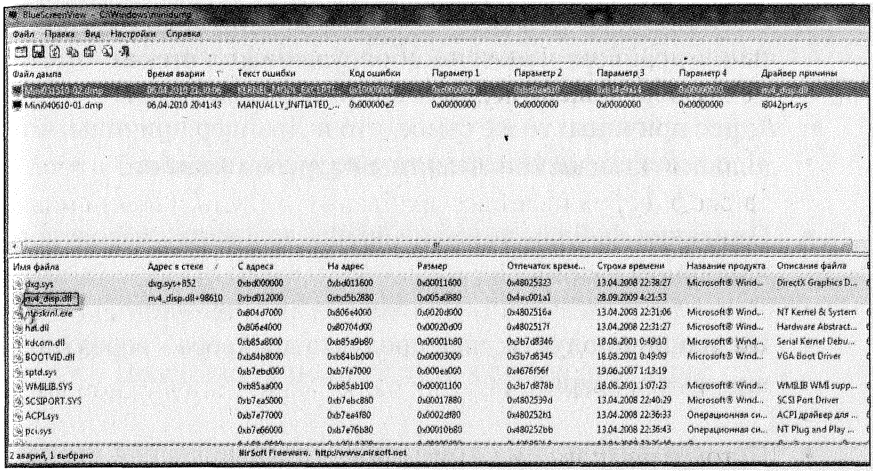


Рис. 9.10. Утилита BlueScreenView

- **Время аварии:** время создания файла, которое соответствует дате и времени совершения ошибки.

- **Текст ошибки:** символьная строка ошибки. Данная строка определяется согласно Коду ошибки и отображается на синем экране.

- **Код ошибки:** код ошибки, как он отображен на синем экране смерти.

- **Parameter 1/2/3/4:** 4 параметра ошибки, как они отображены на синем экране.

- **Драйвер причины:** драйвер, который, вероятно, стал причиной ошибки. BlueScreenView пытается обнаружить истинного виновника аварии в лице драйвера либо модуля, отыскивая его в аварийном стеке. Тем не менее не стоит быть уверенным на все 100% в правильности выбора утилиты. Поэтому вы должны обязательно обратить внима-

ние на нижнюю часть окна утилиты, в которой отображены все драйвера и модули, обнаруженные в стеке.

- **Адрес причины:** то же самое, что и Драйвер причины, но с дополнительным сопоставимым адресом ошибки.
- **Описание файла:** описание файла драйвера - вероятного виновника аварии.
- **Название продукта:** имя продукта драйвера - вероятного виновника аварии.
- **Производитель:** имя компании – производителя драйвера.
- **Версия файла:** версия драйвера – вероятного виновника аварии.

Нижняя часть окна BlueScreenView, в зависимости от настроек в **Options→ Lower Pane Mode,** содержит все драйвера и модули, которые были загружены во время ошибки, либо только драйверы, найденные в стеке. На розовом фоне показаны драйверы, которые, вероятно, вызвали аварию.

- **Имя файла**: имя файла драйвера или модуля.
- **Адрес в стеке**: адрес памяти драйвера в стеке.
- **С адреса**: начальный адрес памяти в стеке.
- **На адрес**: последний адрес памяти.
- **Размер**: размер драйвера в памяти.
- **Отпечаток времени**: отпечаток времени драйвера.

- **Строка времени**: отпечаток времени в формате дата/время.
- **Название продукта**: имя продукта драйвера.
- **Описание файла**: описание файла драйвера.
- **Версия файла**: версия файла драйвера.
- **Компания**: имя компании — производителя драйвера.
- **Полный путь**: полный путь к файлу драйвера.

Нижняя панель может отображаться в трех режимах:

- **Все загруженные драйвера (F6)** – отображение всех драйверов, загруженных во время совершения ошибки, выбранной в верхней панели. При этом драйвера и модули, чья память была обнаружена в стеке, отмечены розовым фоном.
- **Драйверы, найденные в крэш-стеке** (F7) – отображение только драйверов и модулей, чья память была обнаружена в аварийном стеке. В данном режиме велика вероятность того, что один из этих драйверов спровоцировал стоп-ошибку.
- **Голубой экран BSOD в стиле XP (F8)** – отображает синий экран смерти, подобный тому, что вы наблюдали при возникновении стоп-ошибки (рис. 9.11).

Для изменения режимов нижней панели воспользуйтесь меню **Настройки→ Режим нижнего окна** либо быстрыми клавишами. И в заключение хочется отметить, что при определении проблемного драйвера не нужно полагаться только на имя файла в столб-

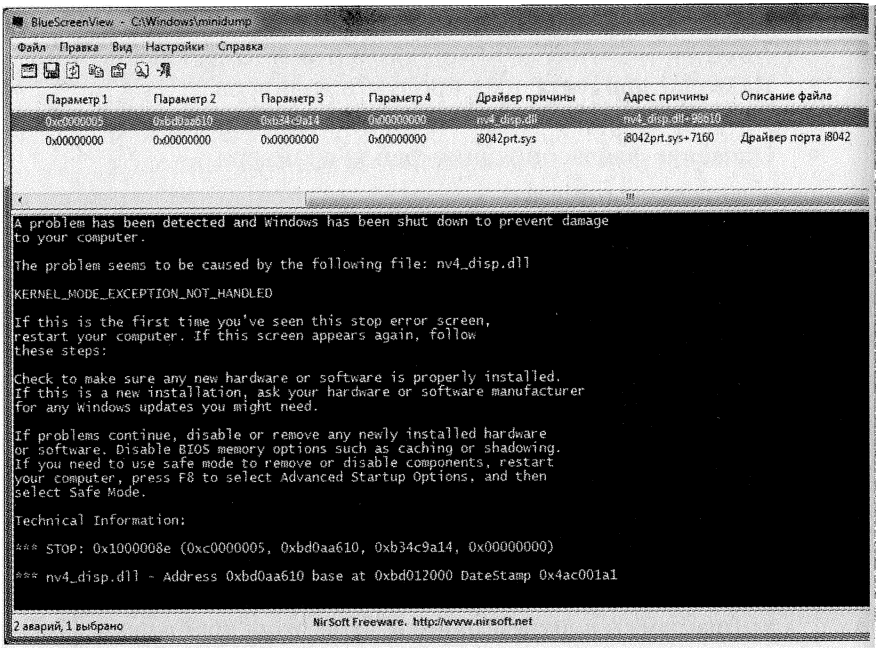


Рис. 9.11. Просмотр дампа в режиме синего экрана смерти

це **Драйвер причины.** Обязательно проанализируйте драйверы нижней части окна утилиты, выделенные розовым цветом. Но главный акцент делайте на несистемные драйверы.

9.5. Искусственное создание синего экрана смерти

Если вы интересуетесь проблемами стоп-ошибок, но они еще не появились у вас во вновь установленной Windows 7 (и лучше бы не появлялись), но вы хотите во всеоружии быть готовым к ним, то вам пригодится данный раздел. Дело в том, что какие бы вы вышерассмотренные настройки дампа памяти ни проводили, ни папки **Minidump**, ни файла **Memory.dmp** вы не обнаружите в своем компьютере. Они появятся лишь после появления пер-

вого сбоя системы, приведшего к синему экрану. Однако разработчиками Windows заранее была подготовлена возможность искусственного вызова BSOD. Зачем? – можете спросить вы. Дело в том, что данной возможностью пользуются разработчики программного обеспечения, а также производители комплектующих к компьютеру для отладки драйверов. Поэтому и вы можете, при большом желании, вручную привести вашу систему к синему экрану. Хотя это бывает иногда даже необходимо, например, для получения файла дампа памяти в определенный момент времени или для авральной остановки системы (на многих современных компьютерах отсутствует кнопка перезагрузки системы Reset). Для инициализации BSOD предварительно необходимо выполнить несколько настроек в системном реестре:

1. Щелкните Пуск и в поисковой строке введите **regedit** и нажмите клавишу **Enter**. Откроется окно редактора системного рееста. Последовательно раскройте ветку HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt**Parameters**.

2. Щелкните правой кнопкой на свободное место в правой области редактора и выберите **Создать→Параметр DWORD (32)** (рис. 9.12). Для 64-битной системы выберите соответствующий пункт.

3. Задайте параметру имя **CrashOnCtrlScroll**.

4. Щелкните по названию нового параметра дважды и установите значение равным 1 (рис. 9.13).

5. Щелкните кнопку ОК. Все. Настроечный этап завершен. Здесь стоит напомнить, что если ранее вы не сняли флажок опции **Выполнить автоматическую перезагрузку,** то синего экрана вы всё равно не увидите. Поэтому снача-

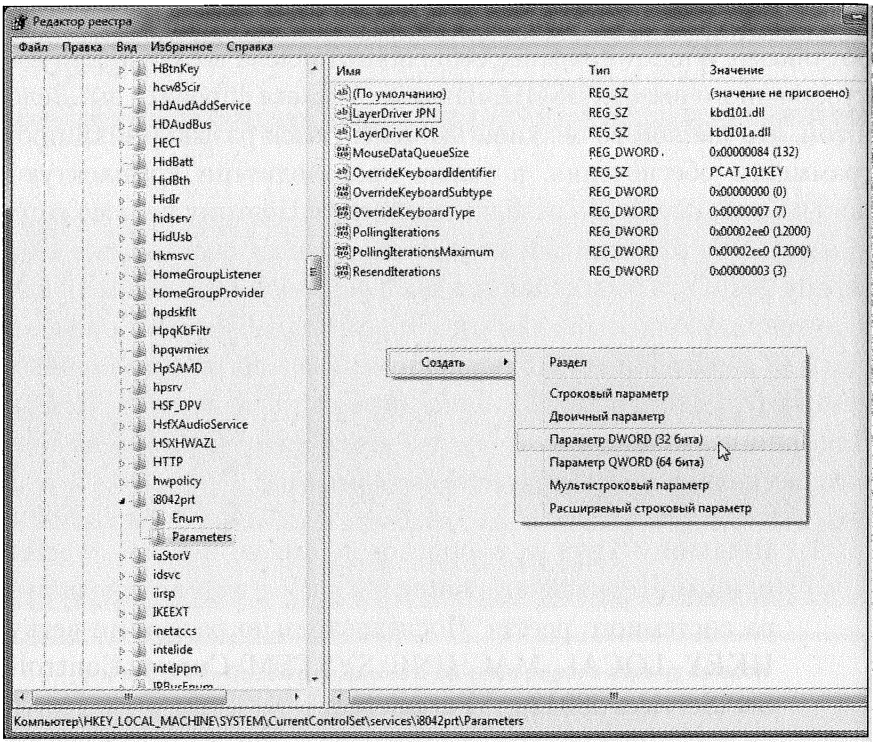


Рис. 9.12. Создание нового параметра

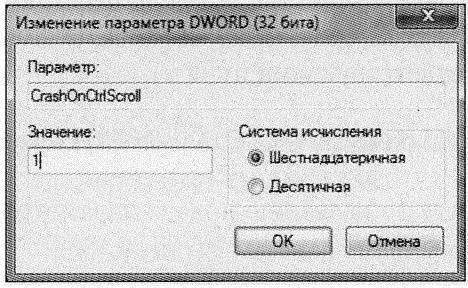


Рис. 9.13. Установка значения параметру CrashOnCtrlScroll

ла отключите данную опцию, как описано выше (см. рис. 9.14).

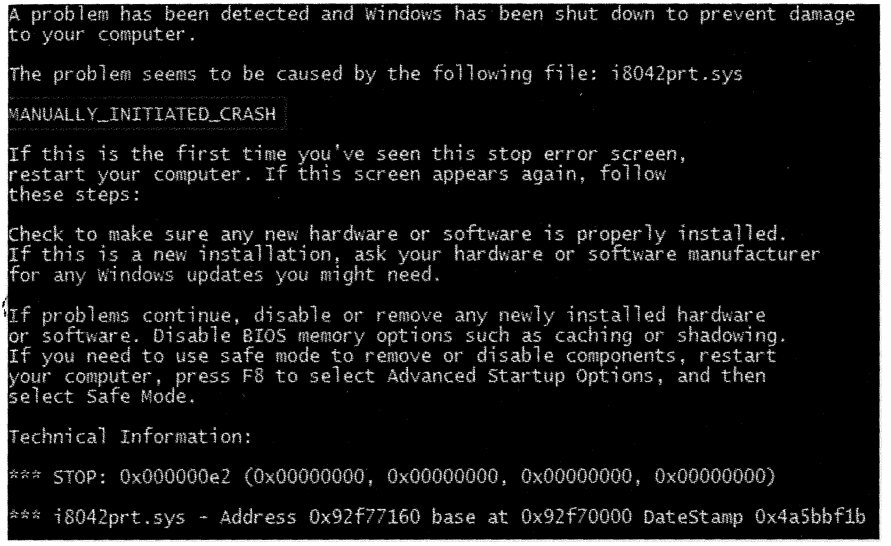


Рис. 9.14. Искусственный BSOD

6. Вызов вручную BSOD осуществляется двойным нажатием клавиши **Scroll Lock**, при этом удерживая клавишу **Ctrl** (Ctrl+Scroll Lock+Scroll Lock). В результате вы получите такую картинку (рис. 9.14).

Кстати, обратите внимание на символьный код ошибки **MANUALLY_INITIATED_CRASH,** что означает вызванную вручную ошибку. Хочется к данной теме еще отметить, что вам не удастся это сделать на USB-клавиатурах, так как они не используют стандартный драйвер *i8042prt.sys.*

9.6. BSOD, да не тот, или о Черном экране смерти

Сразу же после выпущенного 10.11.09. обновления Windows 7, что официально отрицается Microsoft, повсеместно стали проявлять-

ся случаи отображения экрана черным цветом во время процедуры загрузки системы. Панель задач, рабочий стол, кнопка Пуск и все остальное растворилось в черной бездне. Иногда, правда, может отображаться единственное несвернутое окно Проводника. Данная ситуация моментально получила название «Черного экрана смерти», по аналогии с синим собратом.

Кстати, у данного раздела не такой заголовок. Ведь **Black Screen Of Death** по первым буквам получается тоже BSOD. Интересен факт, что Microsoft не очень-то и спешила в выявлении данной тенденции. Но, как это случается, мир не без добрых компаний. Нашлась она и на этот раз. Компанией Prevx была разработана программа, исправляющая причины вызова экрана смерти. Причем после проведенного тщательного расследования появления причины черного экрана Prevx обнародовала его результаты и огласила причины. Было заявлено, что черный экран отображается в связи с особенностями хранения строковых данных в системном реестре.

Не будем загружать ваши головы различными компьютерными терминами, подробно описывая процедуру появления ошибки. Скажем лишь, что Prevx выпустила утилиту **FixShell.exe**. Скачать её можно здесь: http://info.prevx.com/download.asp?GRAB=blackscreenfix . Если вы хотите предотвратить «беду» заранее, то в профилактических целях просто запустите её. Это избавит вас в дальнейшем от черных экранов смерти.

Однако если вы уже испытали данную проблему на себе, то придется выполнить следующий ряд действий. Однако это не сможет гарантировать 100% решения проблемы, так как в системе могут присутствовать различные вредоносные объекты, которые и спровоцировали черный экран. Но все же в большинстве случаев данный метод устранял проблему.

1. Перезагрузите компьютер и выполните вход в систему, при этом вы должны быть подключены к Интернету.

2. Выполните **Ctrl+Alt+Del** и выберите **Запустить диспетчер задач**.

3. Перейдите во вкладку **Приложения**. Щелкните кнопку **Новая задача**. Откроется диалоговое окно **Новая задача**.

4. Введите в поле **Открыть** следующий текст, не забывая о кавычках: **"C:\Program Files\Internet Explorer\iexplore.exe" "http://info.prevx.com/download.asp?GRAB=BLACKSCREENFIX"** (рис. 9.15). Вместо **C:\Program Files\Internet Explorer\iexplore.exe** можно вставить путь к файлу запуска вашего браузера, например **C:\Program Files\Opera\opera.exe** или **C:\Program Files\Mozilla Firefox\firefox.exe**.

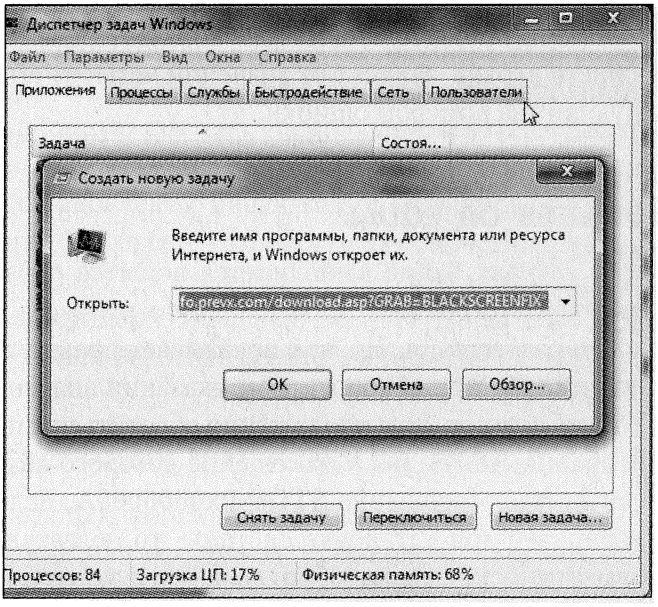


Рис. 9.15. Создание новой задачи

5. Щелкните кнопку **ОК**. Начнется загрузка утилиты.

6. На вопрос **Запустить или сохранить этот файл** щелкните кнопку **Выполнить**. Утилита без вашего участия запустится.

7. Перезагрузите компьютер.

9.7. Список названий самых распространенных стоп-ошибок, приводящих к синим экранам смерти

Ниже мы приведем список самых распространенных BSOD-ошибок, которые вы можете повстречать во время эксплуатации компьютера. Для каждой ошибки мы дадим краткое описание. Следует обратить внимание, что название ошибки не отражает полностью её суть, а дает лишь общее представление о проблемной области, так как очень многие конкретные факторы получения синего экрана зависят от значений четырех его параметров, следующих за номером ошибки.

IRQL_NOT_LESS_OR_EQUAL

Возникает в случаях, когда выполняется попытка обращения к памяти драйвера устройства либо какого-то процесса ядра без данного на то разрешения. Но, как показывает практика, данная ошибка происходит при некорректном указании значения блока памяти. То есть при попытке приложения обратиться к памяти по заранее неправильному адресу, посещение которого для него запрещено, возникает сообщение **STOP 0x0000000A**. Если данная ошибка возникает при установке системы, то обязательно проверьте совместимость вашего оборудования с устанавливаемой системой http://www.microsoft.com/whdc/hcl/default.mspx. Если

вашего устройства нет в списке, обратитесь в службу поддержки производителя оборудования либо в центр разрешения проблем Microsoft. Кроме того, попробуйте проверить драйвер устройства на корректность указания адресов. Для этого воспользуйтесь стандартной утилитой **Диспетчер проверки драйверов**, щелкнув меню **Пуск** и введя в поисковой строке **verifier.exe**. Также может понадобиться обновление драйверов устройств.

APC_INDEX_MISMATCH (STOP: 0x00000001)

К данной ошибке обычно приводит ограниченность в основных ресурсах компьютера, а именно небольшое количество оперативной памяти и ограниченное место на жестком диске. Также может иметь место проблема драйверов устройств.

PFN_LIST_CORRUPT STOP: (STOP: 0x0000004E)

Повреждены input/output структуры драйвера устройства, BIOS либо оборудование компьютера. Попробуйте продиагностировать операционную систему специальными утилитами производителя оборудования. Кроме того, попытайтесь отключить программы восстановления информации, антивирусные сканеры и брандмауэры. Проверьте устройство на совместимость драйверов с Windows 7 http://www.microsoft.com/hcl/default.asp. Сделайте тест RAM, например, с помощью **memtest**. Попытайтесь обновить версию BIOS или сбросить все его настройки.

KMODE_EXCEPTION_NOT_HANDLED (STOP: 0x0000001E)

Довольно распространенная ошибка, связанная с неисправными драйверами или системными сервисами. С помощью утилит «расшифруйте» дамп памяти и выявите основной список драйверов, причастных к появлению критической ошибки. Затем по-

пробуйте отключить, обновить либо удалить «виновников». Другой причиной данной ошибки может послужить несовместимость микропрограммного обеспечения, поэтому попробуйте обновить BIOS вашего компьютера. Если ваш жесткий диск не имеет достаточного свободного пространства, почистите его соответствующими утилитами.

KERNEL_APC_PENDING_DURING_EXIT (STOP: 0x00000020)

В большинстве ситуаций ошибка провоцируется проблемными драйверами. При получении синего экрана с данной ошибкой попробуйте во время загрузки системы, до её появления, нажать F8 и выбрать в списке операций **Загрузка последней удачной конфигурации**. Также попробуйте удалить приложения и драйвера устройств, которые были установлены в последнее время и после появления которых вы и получили синий экран. Если эти действия не принесут пользы, проверьте появления новых релизов драйверов устройств вашего компьютера, в особенности чипсета и видеокарты. Старые драйвера зачастую являются причиной возникновения BSOD.

SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (STOP: 0x0000007E)

Данный синий экран появляется при возникновении нераспознанной ошибки. Иногда драйвер, спровоцировавший ошибку, может быть определен. К рекомендуемым мерам по решению проблемы в Windows 7 можно отнести освобождение дискового пространства путем очистки корзины, уборки компьютера от мусора и удаления ненужных файлов либо переноса их на другие носители или сжатия в архивы. Рекомендуется иметь не менее 1Gb свободной площади жесткого диска. С помощью **Центра обнов-**

ления Windows сделайте все рекомендуемые обновления. Убедитесь в корректности работы драйверов всех устройств компьютера с помощью диагностических программ. При появлении малейшего подозрения на тот или иной аппаратный элемент замените его с целью проверки на устранение данного BSOD. Не поленитесь вручную проверить установку устройств в компьютере, например, правильно ли сидят платы памяти и все ли соединительные провода и кабели хорошо стыкуются между собой. Проверьте устройства на совместимость драйверов с Windows 7, а также наличие их новых версий. Обновите на самую последнюю версию BIOS. Если же ваша текущая версия BIOS является последней, то, возможно, она имеет некорректные параметры, которые являются причиной проблемы. Попробуйте сбросить их. Все настройки хранятся в памяти CMOS. Лучшим способом сброса параметров BIOS является извлечение аккумулятора CMOS. Для этого отключите компьютер и откройте корпус, затем извлеките аккумулятор и подождите чуть более 1 минуты, после чего вставьте его назад. Обычно появляется предупреждение BIOS о повреждении или изменении CMOS, и вам может быть предложено откорректировать системное время и дату.

RUN A SYSTEM DIAGNOSTIC UTILITY SUPPLIED BY... (STOP: 0x1000007F)

На самом деле ошибка занимает несколько строчек текста. Проще её запомнить по коду **STOP: 0x1000007F.** Она означает то, что процессором были обнаружены проблемы, с которыми Windows не смогла справиться. Данная ошибка обычно возникает:

- в случаях дефекта памяти, неправильной её установки либо несоответствия параметров платы памяти конфигурации материнской платы;

- при некорректных настройках BIOS или в случае разгона процессора и памяти;
- в случае перегрева процессора (проблема вентилятора);
- при неисправности оборудования или некорректности драйверов;
- при неисправности процессора (CPU).

Для поиска решения проблемы попробуйте провести следующий ряд операций: с помощью диагностических программ проверьте все оборудование компьютера, в особенности платы памяти и видеоадаптер. Визуально проверьте установку устройств в соответствующие слоты, а также все соединения между оборудованием. Windows 7 имеет в наличии программу тестирования памяти, которая запускается при загрузке с DVD инсталляции Windows 7. Также можно воспользоваться и сторонними продуктами диагностики памяти и видео, например Fix-It Utilities Professional и SystemSuite Professional, а также Eurosoft's PC Check и Iolo's System Mechanic. Проверьте совместимость устройств с материнской платой. Попробуйте загрузить последнюю работоспособную конфигурацию (F8 при загрузке). Кроме того, рекомендуется сделать полное обновление с помощью **Центра обновления Windows**.

NTFS_FILE_SYSTEM (STOP: 0x00000024)

Данная ошибка возникает на NTFS файловых системах. Виновником является файл **Ntfs.sys**, который используется для чтения и записи всех NTFS-драйверов. Для устранения проблемы необходимо проверить диск на наличие ошибок. Для этого одновременно нажмите кнопки **Windows+E**. Выберите жесткий диск и щелкните его правой кнопкой мыши. Выберите пункт **Свойства**. В открывшемся окне **Свойства** перейдите в папку **Сервис** и щелкните

кнопку **Выполнить проверку**. Откроется диалоговое окно **Проверить диск**, где установите флажок **Автоматически исправлять системные ошибки**. Вторую опцию можете оставить без флажка, но можете и включить её, но при этом проверка будет проводиться достаточно дольше (рис. 9.16).

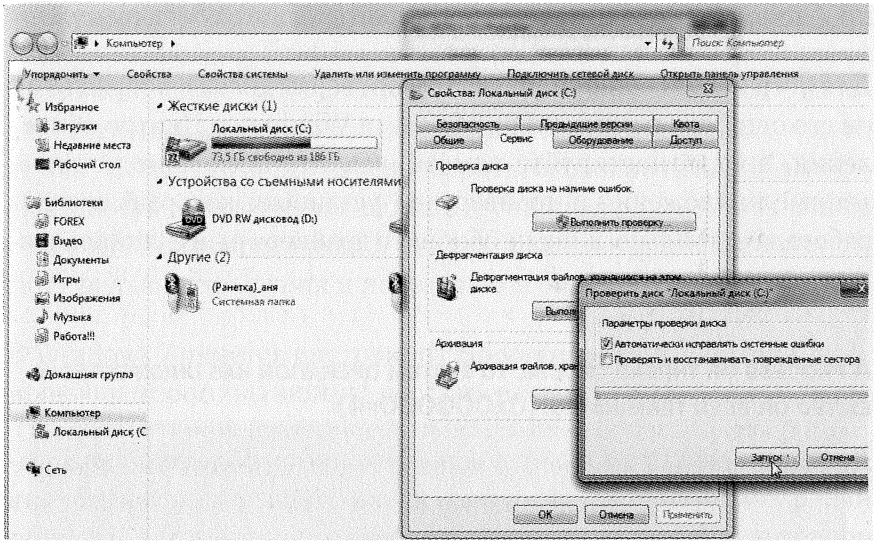


Рис. 9.16. Запуск проверки жесткого диска

Щелкните кнопку **Запуск.** Начнется проверка с одновременным исправлением дисковых ошибок. Кроме проверки диска, выполните процедуру обновления Windows. Для полноценной работы операционной системы, а также запуска различных приложений может не хватать используемой оперативной памяти, поэтому рекомендуется при её нехватке установить дополнительные модули. Также данная ошибка может возникнуть при физических неполадках корпуса диска, а также его контроллера. Поэтому тщательно проверьте надежность подключения кабеля (шлейфа).

PAGE_FAULT_IN_NONPAGED_AREA (0x00000050)

Данная надпись на синем экране возникает при попытке доступа к памяти по некорректному адресу в связи с ошибкой драйвера. Кроме того, эта ошибка может появиться при возникновении проблемы с оборудованием, повреждением тома NTFS и даже проблемой работы антивирусного программного обеспечения.

Для устранения ошибки проведите проверку диска с исправлением его ошибок (см. рис. 9.16), обновите Windows в **Центре обновления**, продиагностируйте память, удалите последние установленные приложения и драйвера, до установки который система работала стабильно, а также обновите драйвера ранее установленных устройств.

A PROCESS OR THREAD CRUCIAL TO SYSTEM OPERATION HAS UNEXPECTEDLY EXITED OR BEEN TERMINATED. (0x000000F4)

Данная ошибка возникает в основном при проблеме оборудования, а конкретней, загрузочного диска. Проверьте правильность подключения жестких дисков (особенно системного) к материнской плате. Проверьте корректность установок джамперов (Master/Slave) и другие настройки, в зависимости от типа подключаемого жесткого диска.

Также попробуйте обновить драйвера устройств. Если рекомендуемые действия не будут увенчаны успехом, а вы имеете ранее созданный образ диска, то можно сделать полное восстановление системы, при котором все новые данные пропадут. Но если найти чистый жесткий диск и на него «наложить» образ старого диска, то вы можете проверить, в чем же заключается проблема. Если новый диск будет работать, то дело в неисправном старом диске. Если и новый диск откажется работать, то проблема в соединениях на материнской плате либо в кабелях.

PROCESS1_INITIALIZATION_FAILED (STOP: 0x0000006B)

Возникновение этой ошибки означает появление проблем в структуре запуска Windows. При этом невозможно войти в Windows ни обычным путем, ни с помощью Безопасного режима, ни с помощью загрузки Последней удачной конфигурации. Поэтому вам остается выполнить следующие действия, чтобы попытаться восстановить систему. Если вы прямо перед возникновением ошибки проводили какие-либо действия с жесткими дисками, то с большой степенью уверенности можно сказать, что вы сделали что-то не так. Попробуйте все перепроверить, особенно правильность и надежность подключения кабелей и установку джамперов. Затем с помощью диагностических утилит просканируйте жесткие диски с целью нахождения и исправления ошибок.

В Windows 7 имеется инструмент **Восстановление системы**, с помощью которого вы можете восстановить отсутствующие или за-

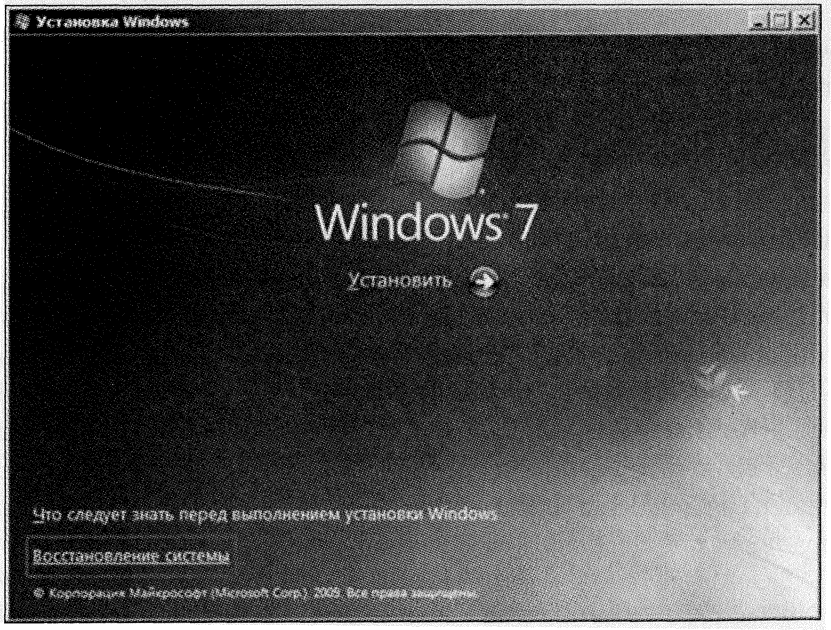


Рис. 9.17. Выбор пункта Восстановление системы

менить поврежденные файлы. Для этого потребуется установочный DVD Windows 7. В начале установки вам нужно будет выбрать не **Установить**, а **Восстановление системы** (рис. 9.17).

Откроется окно с различными вариантами дальнейших действий (рис. 9.18).

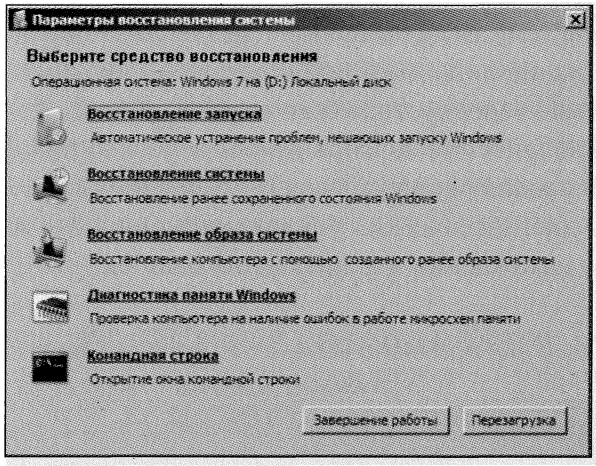


Рис. 9.18. Варианты восстановления системы

DRIVER_IRQL_NOT_LESS_OR_EQUAL (STOP: 0x000000D1)

Одна из самых распространенных ошибок. Драйвер устройства содержит ошибку, поэтому пытается получить доступ к памяти по некорректному адресу. Также может быть испорчен файл подкачки, либо имеются проблемы памяти. Для решения проблемы попытайтесь выполнить все обновления системы. Если вы используете несколько контроллеров RAID Mylex с драйвером Dac2w2k.sys, то обновите RAID драйвера. Читайте здесь http://support.microsoft.com/?kbid=316208. Также выполните тест памяти, с помощью инструмента Диагностика памяти компьютера (см. рис. 9.18). Попробуйте удалить последние установленные приложения и драйвера.

В случае с файлом подкачки выполните следующее. Во-первых, данный файл может быть поврежден, поэтому удалим его. Загру-

зитесь с помощью установочного диска Windows 7 и перейдите в окно выбора операций восстановления (см. рис. 9.18). Выберите пункт **Командная строка**. В системной папке **(C:\)** введите **del pagefile.sys.** Запустите проверку и исправление диска с помощью команды **chkdsk /r.** Покиньте консоль восстановления и перезагрузите систему. Теперь вы нуждаетесь в создании нового файла подкачки, поэтому щелкните **Пуск→**, а затем правой кнопкой **Компьютер→Свойства.** Щелкните **Дополнительные параметры системы**. В открывшемся окне **Свойства системы** перейдите в папку **Дополнительно**. Щелкните кнопку **Настройка** в разделе Быстродействие. Откроется окно **Параметры быстродействия**, где перейдите во вкладку **Дополнительно**. Щелкните кнопку **Изменить**. Дальнейшие действия по настройке виртуальной памяти мы рассматривали ранее (см. рис. 9.3).

BAD_POOL_CALLER (STOP: 0x000000C2)

Возникает в случае неверного запроса памяти приложением или драйвером. Выполните тест памяти с помощью встроенной утилиты Windows 7 **Диагностика памяти компьютера** (см. рис. 9.18). Кроме того, проверьте совместимость параметров модулей с параметрами материнской платой. Если вы заменили или добавили новые модули перед самым возникновении ошибки, то попробуйте заменить их на старые и посмотреть на результат. Также проверьте, насколько плотно модуль «сидит» в слоте материнской платы. Сделайте обновление Windows и драйверов устройств.

При возникновении данного BSOD может потребоваться переустановка системы, при этом вы можете потерять все ваши данные. Поэтому рекомендуется (по возможности) сделать самую свежую копию ваших данных перед началом переустановки.

RUN A SYSTEM DIAGNOSTICS SUPPLIED BY YOUR... (STOP: 0x0000002E)

В старых версиях Windows ошибка отображалась как DATA_BUS_ERROR. Возникает при ошибке памяти. Сбой контроля четности указывает на неполадки оборудования. Как правило, это относится к основной памяти либо видеопамяти. Для устранения неполадки комплексно проверьте память (тест+визуальный осмотр), обновите последние драйвера видеоадаптера, а также проверьте его на соответствие с конфигурацией материнской платы (для внешней видеокарты).

REMOVE ANY RECENTLY INSTALLED SOFTWARE...(STOP: 0x0000003F)

Нехватка оперативной памяти для надлежащей работоспособности устройства. Требуется дополнительная память. Основным решением проблемы, естественно, является увеличение объема оперативной памяти (по возможности) либо уменьшение количества запускаемых одновременно программ, в особенности тех, которые работают в фоновом режиме. Если ваш видеоадаптер не имеет собственной памяти и использует основную память компьютера, то попробуйте ограничить её максимальный размер. Это особенно актуально для недорогих ноутбуков.

KERNEL_STACK_INPAGE_ERROR (STOP: 0x00000077)

Windows не может прочитать файл с диска. Это могут быть поврежденные сектора, проблемы оборудования (диск, контроллер, память), вирусное заражение либо ошибка в драйвере устройства. Для обнаружения проблемного участка компьютера начните с комплексного изучения памяти (тест+визуальный осмотр), затем обновите самыми последними базами антивирусную программу и проверьте свою систему на наличие вредоносных объектов. Если вы недавно меняли, добавляли либо удаляли жесткие диски или

кабели к ним, то возможно, что что-то сделано неправильно. Перепроверьте, что диски установлены должным образом, а кабели не перепутаны. Подключение шлейфов дисков к другим разъемам материнской платы либо изменение джамперов master/slave (на старых ATA-дисках) могут привести к проблеме. Существует возможность выхода из строя диска, поэтому проверьте его средствами диагностики или подключите к компьютеру другой диск, чтобы убедиться в работоспособности других устройств компьютера.

В заключение обновите систему с помощью Центра обновления. Рекомендуется обновить даже необязательные обновления. То же самое выполните и для драйверов устройств.

THE DRIVER HAS USED AN EXCESSIVE NUMBER OF OF SYSTEM PTEs. (STOP: 0x000000D8)

Драйвер устройства имеет ошибку и не очищает должным образом память. Проблема может быть вызвана несколькими драйверами одновременно. Иногда имена драйверов будут отображены на синем экране. При получении данного BSOD сначала проверьте наличие обновлений для драйверов устройств вашего компьютера, в особенности чипсета и видеоадаптера. Получите все последние обновления Windows, а также удалите все недавно установленные приложения и драйвера, до установки которых данная критическая ошибка не наблюдалась.

THE DEVICE DRIVER GOT STUCK IN AN INFINITE... (STOP: 0x000000EA)

Драйвер устройства имеет ошибку, приводящую процесс к бесконечному циклу. Обычно данная проблема возникает у видеоадаптеров. Поэтому попробуйте сначала обновить видеодрайвера до самой последней версии. Затем с помощью диагностических утилит определите работоспособность устройств. В случае, если вы заподозрите какое-либо устройство, например карту памяти или видеоадаптер, то по возможности замените его другим,

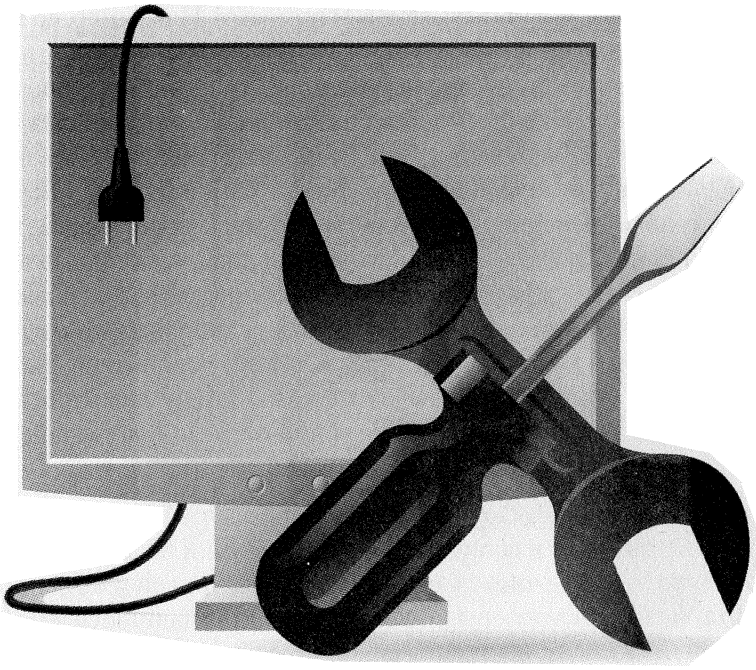
про который вы точно знаете, что он работает. Проверьте устройства на совместимость с Windows по ссылке Windows Hardware Compatibility List. Обязательно визуально проверьте, как установлены устройства в слотах материнской платы. Соответственно, сделайте обновления Windows и драйверов устройств.

STATUS_SYSTEM_PROCESS_TERMINATED (STOP: 0xC000021A)

Ошибкой приложения, драйвером устройства либо восстановлением непригодного системного файла была нарушена безопасность Windows. Например, если у вас установлено приложение GoBack, которое входит в состав Symantec System Works, то вы должны удалить данную версию, так как она не совместима с системой. Как это выполнить, рассмотрено в статье http://support.microsoft.com/?kbid=318666. Использование старых версий IE тоже может привести к данной проблеме. Обновите браузер IE до текущей версии. Кроме этого, вы можете попробовать загрузить последнюю удачную конфигурацию, щелкнув «F8» при загрузке системы. Обновите Windows последними пакетами обновления. Если вы имеете резервную копию либо образ диска, то отформатируйте диск и восстановите систему. Либо если вы имеете запасной жесткий диск, то установите его на место старого и выполните инсталляцию системы. Этим вы сможете удостовериться, аппаратная или программная ошибка является источником проблемы.

ГЛАВА 10.

НЕ ЧИТАЕТСЯ ДИСК CD ИЛИ DVD. КАК ВОССТАНОВИТЬ ДАННЫЕ С «ПЛОХИХ» ДИСКОВ



10.1. Подбор привода

Самым слабым звеном лазерных дисков является привод. По статистике, в трех случаях из пяти именно он виноват в том, что информацию не удается извлечь в штатном режиме. Причины, по которым это происходит, могут быть самыми разными. Например, со временем сбивается юстировка оптики или уменьшается мощность лазера. Грязь, попавшая на посадочную площадку шпинделя, способна привести к таким биениям вставляемого диска, что система фокусировки просто не успевает установить оптимальное положение линзы. Весьма частое явление — загрязнение самой линзы. Широко распространено мнение, что лучше всего диск воспринимает то устройство, на котором он был записан. Увы, практика показывает, что это не так. Опытные компьютерные пользователи, которым по роду занятий приходится часто иметь дело с «капризными» носителями, обычно долго подбирают, а затем бережно используют дисковод. Иногда такой привод подключают к компьютеру лишь для чтения проблемного диска, а в остальное время отсоединяют шлейф во избежание лишнего износа.

Факторов, влияющих на работу привода, чрезвычайно много: это и точность изготовления и сборки механики и оптики, и конструктивные особенности, в том числе механизмы балансировки и компенсации люфта, и свойства лазерного излучателя, и особенности микропрограммы... Даже если вы и найдете полное описание технических параметров, то разобраться в нем вряд ли сможете. Поэтому приходится полагаться на честное имя производителя и некоторые характеристики.

Согласно эмпирическому правилу, о качестве привода CD или DVD можно судить по его цене и массе (в дешевых моделях ради экономии металлические детали часто заменяют на пластиковые).

Другая немаловажная характеристика — доступный диапазон скоростей чтения. В общем случае — чем ниже скорость вращения диска, тем мягче требования, предъявляемые к его качеству. Правда, зависимость эта не всегда линейна. Большинство приводов имеют одну или несколько наиболее предпочтительных скоростей вращения, на которых их читабельная способность максимальна. Например, на скорости 16x дефектный диск читается «на ура», а на всех остальных скоростях (скажем, 2x, 4x, 8x, 32x) — не распознается вообще. Предпочтительная скорость легко определяется экспериментально, необходимо лишь перебрать полный диапазон доступных настроек.

При покупке CD-ROM'а выбирайте тот привод, у которого скоростной диапазон максимален. Отсутствие скоростей порядка 4x–8x ограничивает «рацион» привода только высококачественными дисками.

По непонятным причинам штатные средства операционной системы Windows не позволяют управлять скоростью диска и потому прихо-

CD/DVD-привод

дится прибегать к помощи сторонних утилит, на недостаток которых, впрочем, жаловаться не приходится (достаточно назвать Slow CD и Ahead Nero Drive Speed). В принципе, большинство приводов самостоятельно снижают скорость, натолкнувшись на нечитаемые сектора, однако качество заложенных в них алгоритмов все еще оставляет желать лучшего, поэтому «ручное» управление скоростью дает значительно лучший результат.

10.2. Механические повреждения дисков и как от них избавиться. Полировка

На лазерных дисках физические проблемы, кроме деградации слоев, почти всегда видны невооруженным взглядом. Осмотр нечитаемого диска при хорошем освещении и под разными углами позволяет сразу выявить сколы, трещины, потертости и царапины. К физическим загрязнениям можно отнести и появляющиеся вследствие неаккуратного обращения загрязнения. К слову, обычная очистка зачастую оказывается эффективнее, нежели опасные манипуляции со шлифовкой и полировкой диска.

Лучше всего справляются с удалением грязи с поверхности диска специальные нетканые салфетки, смоченные очищающим раствором. Мягкую ткань нецелесообразно использовать из-за того, что она оставляет ворсинки, а бумажные салфетки (кроме тех, что предназначены для оптики) царапают защитное пластиковое покрытие.

Помимо фирменных растворов подходят бытовые стеклоочистители, слабые (0.5–1%) эмульсии моющих средств, водный раствор этилового или изопропилового спирта с концентрацией от 10 до 40%. При протирании диска движения должны быть направлены радиально — от центра к краям. Иногда рекомендуют сначала очистить диск тряпкой с раствором, а потом промыть под струей воды и обсушить салфеткой.

Теперь поговорим о более грубых физических дефектах. Самым серьезным среди них следует признать сквозные трещины. Они могут

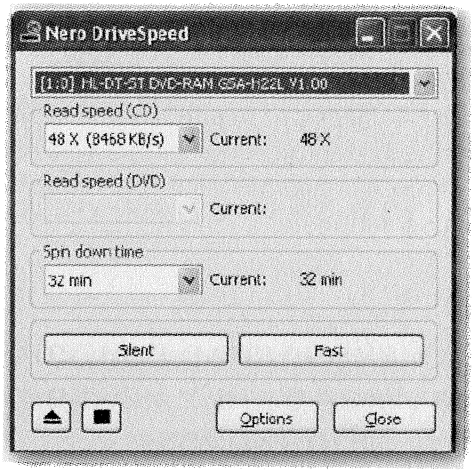


Рис. 10.1. Для снижения скорости вращения диска необходимо применять специальные утилиты

повредить не только данные, но и работающий привод (под действием центробежных сил диск вполне способен разорваться на части).

Бороться с трещинами, заливая их клеем или иным способом укрепляя диск, практически бесполезно — возникающие за счет внутренних напряжений расхождения краев трещин превосходят допустимую ошибку позиционирования луча. Однако если вы приклеите с верхней стороны скотч или пленку типа «Оракал», то по крайней мере предотвратите разлет осколков. Дополнительной гарантией безопасности станет уменьшение скорости вращения шпинделя посредством программных средств (например, программы Nero Drive Speed — см. рис. 10.1).

Довольно много неприятностей способны доставить и царапины. Наиболее уязвима верхняя сторона: легко преодолев тонкое лаковое покрытие, механические повреждения необратимо уничтожают фрагменты отражающего или записываемого слоев. Кстати, к такому же печальному итогу нередко приводит нанесение надписей первым попавшимся маркером.

Дефекты поликарбонатной пластины не столь опасны. Например, немногочисленные узкие царапины не должны вызывать никакого

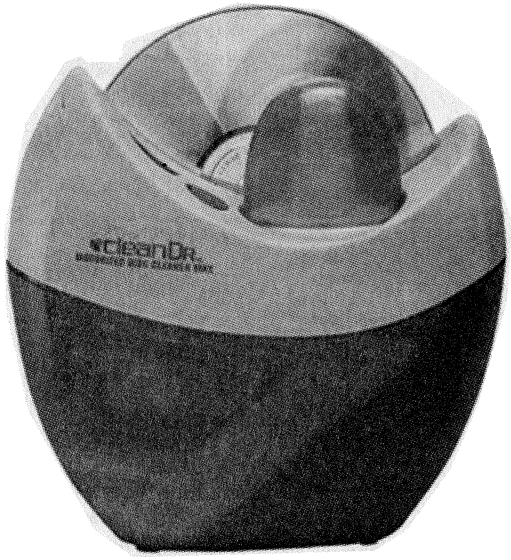


Рис. 10.2. CleanerDR — чистка диска. /Принцип работы устройства - полировка поверхности компакт-диска. С диска снимается верхний слой пластика, в результате чего царапины либо исчезают вовсе, либо становятся менее глубокими, что уменьшает преломление лазерного луча и восстанавливает "читабельность" диска. Самое интересное, что цена этого устройства совсем невелика - всего лишь $20. Если оно действительно работает именно так, как заявлено, то такую штуку должен иметь дома каждый [8]

беспокойства: содержимое сектора «размазано» вдоль спиральной дорожки и потому выпадение нескольких байт легко компенсируются за счет избыточности. Другое дело — широкие царапины: мало того, что они «съедают» несколько фреймов целиком, так еще и сбивают оптическую головку с дорожки. Попав в своеобразную дыру, головка совершенно дезориентируется (ей становится попросту не на что опираться!) и «вылетает» в одну из соседних дорожек. Умные приводы автоматически распознают такую ситуацию и возвращают головку на нужное место, однако менее сообразительные модели (коих, кстати, подавляющее большинство) самоуверенно продолжают чтение как ни в чем не бывало. В результате голова одного сектора скрещивается с хвостом другого и, естественно, при попытке восстановления такого сектора штатными корректирующими кодами

Рис. 10.3. Наибольшую опасность представляют концентрические царапина (по кругу), поэтому протирать диски рекомендуется от центра к краю

ничего, кроме мусора, не получается, и привод уныло диагностирует неисправимую ошибку. Выход — читать такой сектор до тех пор, пока головка не попадет на ту же самую дорожку, с которой начиналось чтение сектора. Количество попыток чтения при этом должно быть достаточно велико (от 100 и больше), ведь с точки зрения вероятности отклониться от спиральной дорожки намного проще, чем удержаться на ней!

Концентрические царапины — самый деструктивный из всех возможных типов разрушений. Дело в том, что они затеняют участки на дисках так, что микропрограмма привода оказывается бессильна их восстановить, основываясь на избыточных кодах коррекции ошибок. К тому же концентрические царапины сбивают систему слежения.

Рис. 10.4. Набор для ручной полировки диска

В теории справиться с царапинами на нижней стороне диска не составляет труда. Существует два способа:

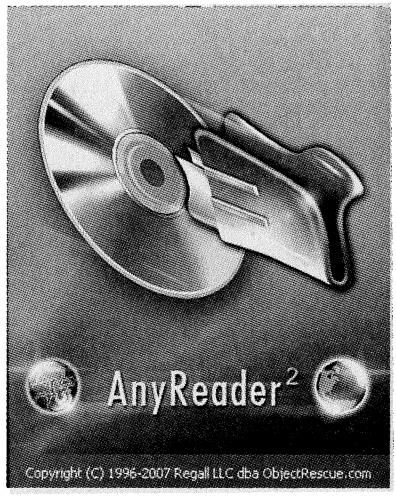
- заполнить углубления материалом с близким к поликарбонату коэффициентом преломления;
- равномерно отшлифовать поверхность пластины до дна самых глубоких дефектов, а затем отполировать ее.

Способам полировки оптических поверхностей (и лазерных дисков в частности) посвящено огромное количество статей, опубликованных как в печатных изданиях, так и в Интернете. Действительно, поцарапанный диск в большинстве случаев можно отполировать, и, если все сделать правильно, вернуть из небытия. Но, во-первых, по-

Рис. 10.5. Народные уменьцы полируют диски зубной пастой.

лировка восстанавливает лишь царапины нижней поверхности диска и бессильна противостоять разрушениям отражающего слоя. Во-вторых, устраняя одни царапины, вы неизбежно вносите другие — после иной полировки состояние лазерного диска может очень сильно ухудшиться. В-третьих, полировке дисков невозможно научиться за раз — вам понадобится уйма времени и куча «подопытных» дисков. Одним словом, восстанавливать диски таким способом имеет смысл в том случае, если вы владеете салоном видеопроката — иначе окупить потраченные деньги, усилия и время не удастся.

10.3. Программное восстановление данных



В названии данного раздела слово «домохозяйка» вынесено с той лишь целью, дабы подчеркнуть нацеленность данной программы AnyReader на определенную пользовательскую аудиторию – «чайники». Это не значит, что программа плоха или хороша, это просто говорит о том, что, чтобы пользоваться ею, вам не понадобится никаких предварительных навыков. Тем более что интерфейс у программы русскоязычный. Программу можно бесплатно использовать 30 дней с максимальным ограничением общего объема восстанавливаемых файлов 700 Мб.

Вся работа в программе AnyReader (www.anyreader.com) строится в виде вопросов и ответов для Мастера, а сам процесс занимает пять-шесть шагов:

1. Вставьте проблемный диск CD (или DVD) в ваш привод. Запустите программу AnyReader. Взглянув на окно приветствия, сделайте умный вид и со знанием дела нажмите **Далее**. В результате появится следующее окно, в котором вам будет предложено выбрать одну из четырех задач (рис. 10.6):

- **Копирование файлов с поврежденных носителей** – предназначена для копирования файлов независимо от их расположения (CD, DVD, флешка, раздел жесткого диска). Практическая применимость данного пункта сомнительна, так что опустим ее.
- **Копировать информацию с поврежденных CD/DVD/BlueRay/HDDVD** – это то, что нам нужно в рамках нашей задачи.
- **Копирование файлов с нестабильных сетей** – позволяет облегчить жизнь в тех случаях, когда вы что-то пытаетесь скачать, ра-

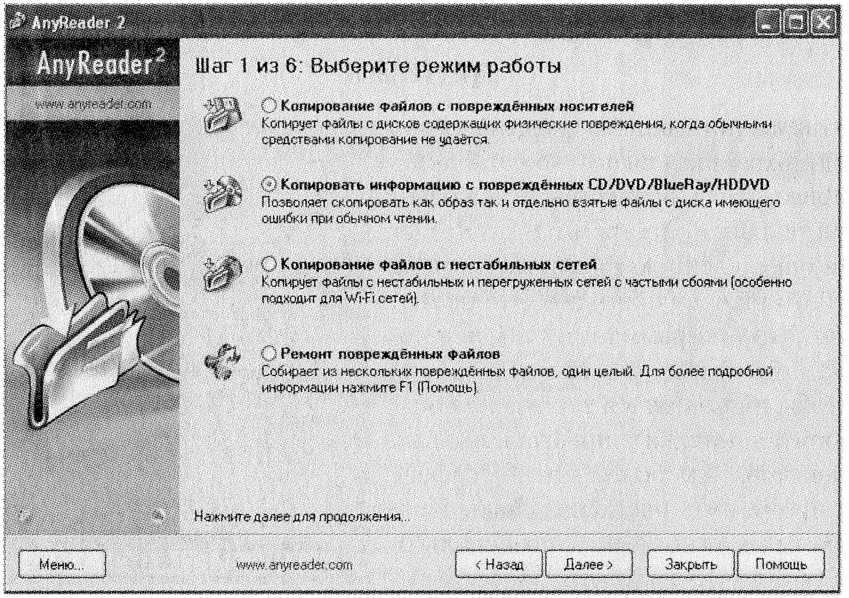


Рис. 10.6. Программа AnyReader: старт

ботая в весьма нестабильной сети (например, в перегруженной беспроводной сети Wi-Fi, сигнал которой очень плохой).

- **Ремонт поврежденных файлов** – на основе нескольких нерабочих копий одного и того же файла попробует воссоздать исходный файл.

2. Установим переключатель в положение **Копировать информацию с поврежденных CD/DVD/BlueRay/HDDVD** и нажмем **Далее.**

3. На следующем этапе нужно указать, что вы хотите: попытаться скопировать отдельные файлы с диска – **Копировать файлы** – или создать образ диска – **Копировать образ диска**. Создание образа в рамках данной программы бессмысленно, так как она не умеет с ними работать. А те программы, которые это дело разумеют, и сами умеют создавать образы. Поэтому выбираем **Копировать файлы** и жмем кнопку **Далее** (рис. 10.8).

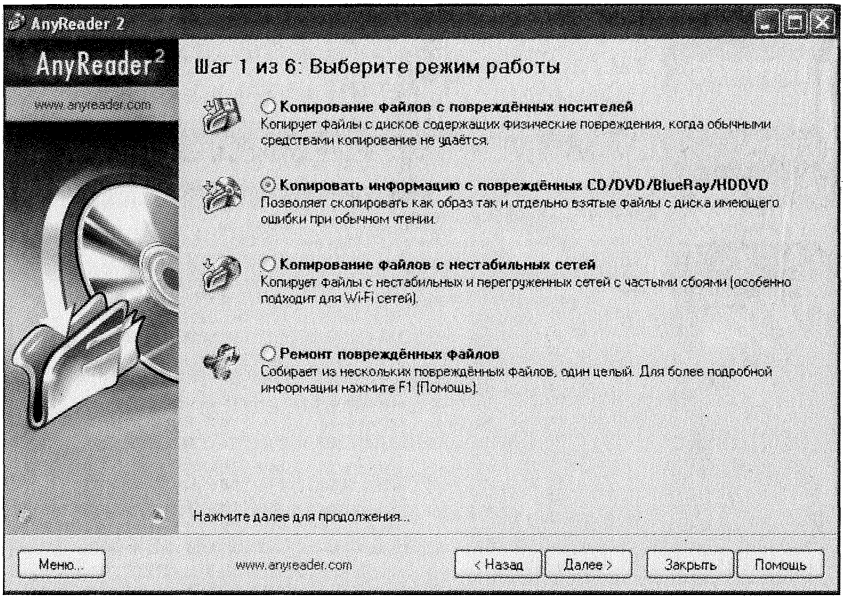


Рис. 10.7. Программа AnyReader: выбор действия

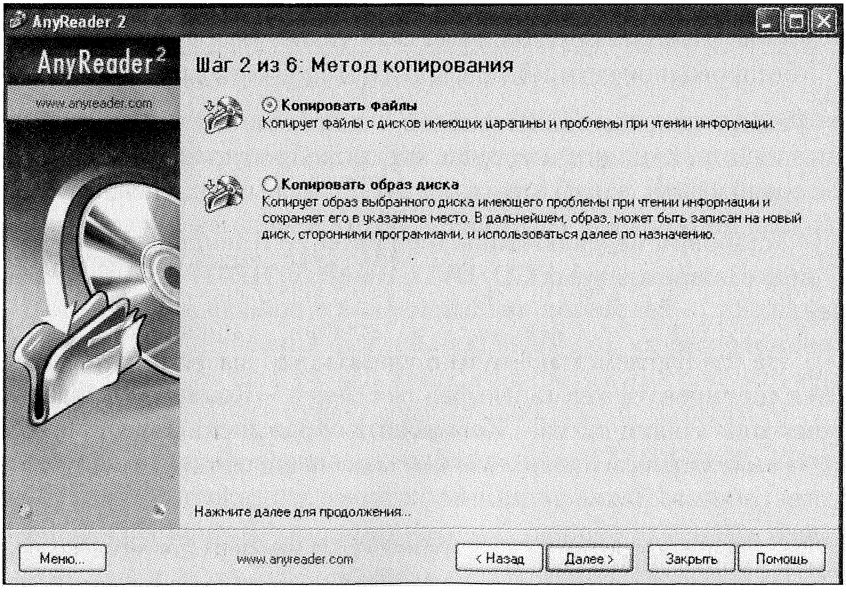


Рис. 10.8. Выбираем «Копировать файлы»

4. Теперь перед вами появится дерево папок вставленного в привод диска. Проставьте галочки напротив тех файлов и папок, которые вам требуется извлечь (рис. 10.9). Закончив, нажмите **Далее**.

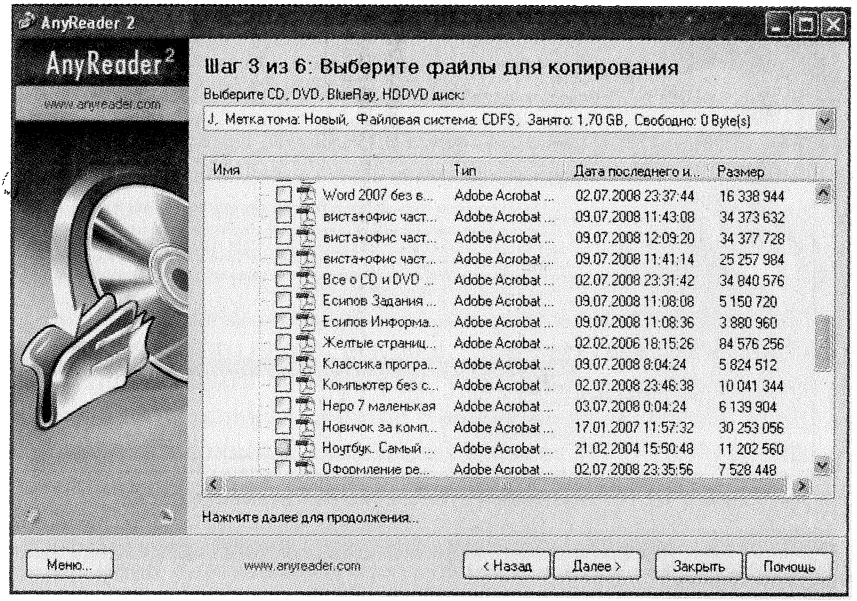


Рис. 10.9. Дерево файлов и папок лазерного диска

5. В следующем окне Мастера от вас потребуется задать параметры копирования, с которыми программа будет пытаться извлечь файлы с диска. Нажав кнопку **Обзор**, укажите папку, в которую должно быть произведено восстановление. В раскрывающемся списке **Степень поврежденности носителя** укажите, насколько вы оцениваете поврежденность вашего диска. В соответствии с вашим выбором автоматически будут установлены оптимальные значения в поле **Количество попыток чтения битого сектора** и в поле **Пауза между попытками чтения битого сектора**. В то же время вы можете сами вручную задать их значения. Можно поэкспериментировать с разными значениями. Нажмите **Далее**.

6. За ходом копирования вы сможете наблюдать в окне программы. По окончании отобразится финальное окно, в котором вам пред-

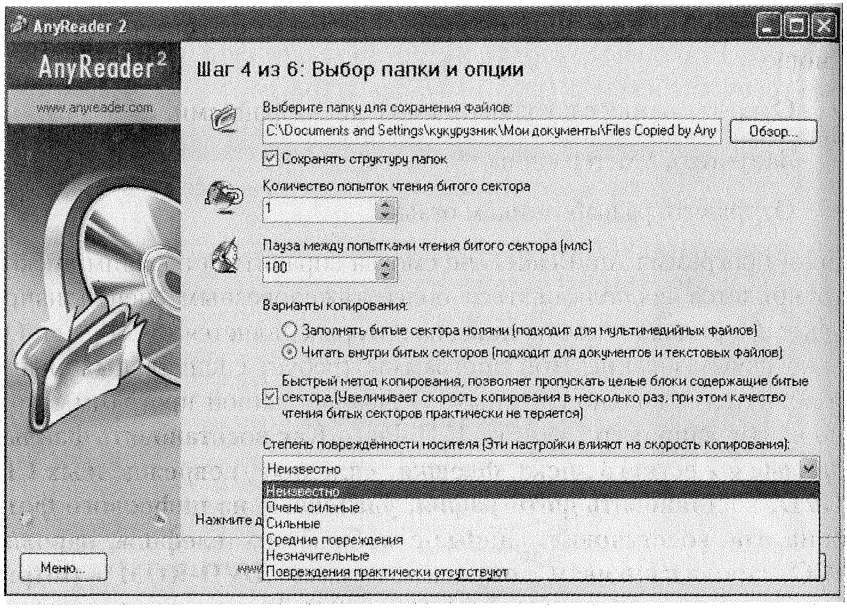


Рис. 10.10. Указываем степень поврежденности диска

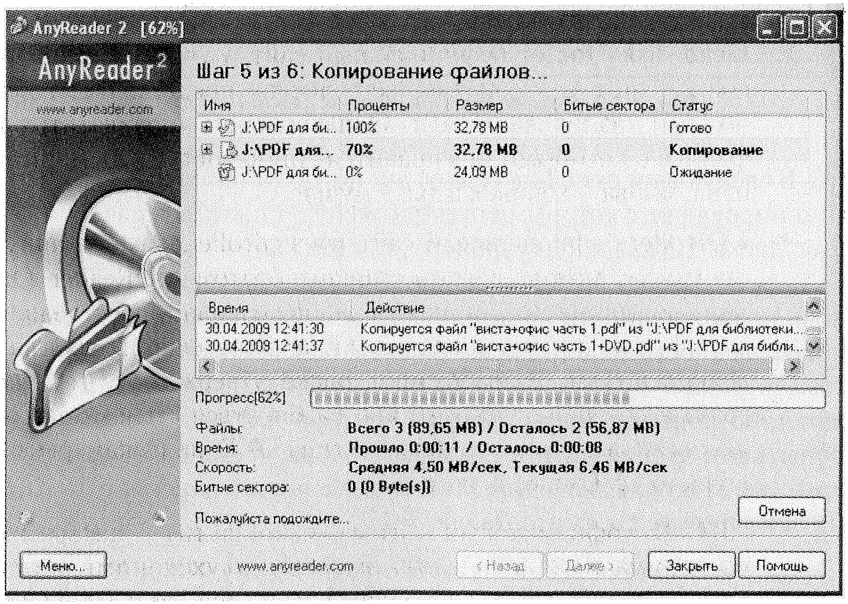


Рис. 10.11. Идет процесс считывания

ложат выбрать одно из трех действий, нажав на соответствующую кнопку:

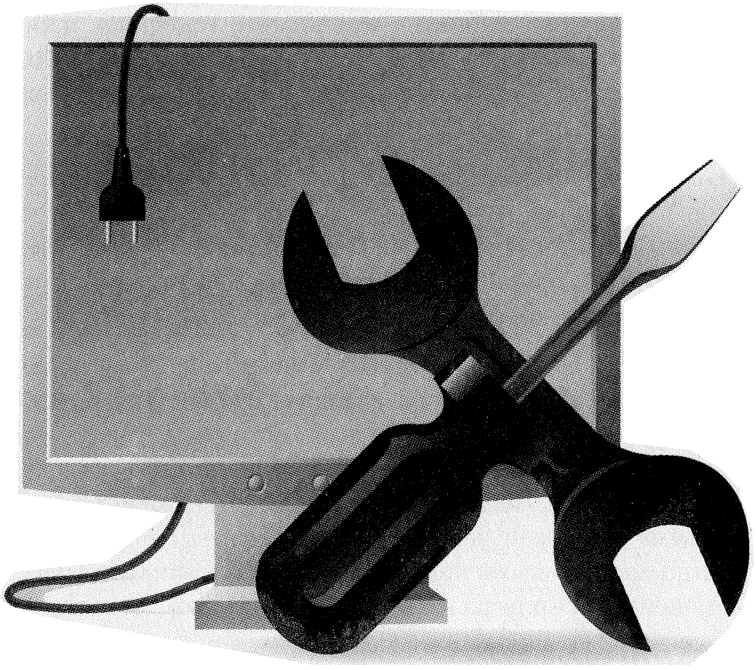
- Открыть папку с сохраненными с диска файлами.
- Запустить Мастер снова.
- Отправить разработчикам отзыв.

Если программа AnyReader не смогла справиться с вашим диском, то придется воспользоваться более тяжеловесным специализированным приложением, лучшим из которых является ISO Buster. Однако использование этой программы требует специальных знаний и является довольно сложным. Описание данной программы можно найти, например, в книге К.П. Рец. **«Как восстановить файлы и данные с жесткого диска, флешки, «плохих»/поврежденных CD/DVD, восстановить фотографии, удаленные из цифрового фотоаппарата, восстановить данные с мобильного телефона, пароли к ICQ, пароли к архивам, документам и т.д. (+ DVD-ROM)» (http://www.ozon.ru/context/detail/id/4625002/)** Также хочется перечислить еще несколько программ, аналогичных AnyReader:

- **Dead disk Doctor** (официальный сайт www.deaddiskdoctor.com) – этот «доктор умершего диска» представляет собой полный аналог AnyReader. Однако может «подхватить» те файлы, с которыми не справится AnyReader. Как говорится одна голова – хорошо, а две – лучше.
- **CDRoller** (официальный сайт www.cdroller.com) – данную программу можно считать старшим братом AnyReader. Она помимо чтения проблемных файлов позволяет восстанавливать файлы с утраченных сессий, а также еще проделывать всякие штуки. Разработчики также утверждают, что программа позволяет эффективно разбираться с дисками, созданными бытовыми приборами типа DVD-видеокамеры, пишущего DVD-плеера и т.п.
- **АКОЛЬ** (официальный сайт www.akol.int.ru) – интересная программа восстановления, имеющая двухоконный интерфейс наподобие файлового менеджера типа Far и Total Commander.

ГЛАВА 11.

КОМПЬЮТЕР ПОСЛЕ ВКЛЮЧЕНИЯ «ПИЩИТ» И НЕ ЗАГРУЖАЕТСЯ



11.1. Что это за звуки?

У вас при включении компьютера сначала появляется служебная информация, потом раздаются «пищащие» звуки-гудки, а потом ничего не происходит (загрузка компьютера прерывается). А возможно вообще на экране ничего не происходит, а просто раздаются гудки.

Гудки означают, что у вас неполадки с каким-либо важным устройством внутри компьютера. При включении компьютер произ-

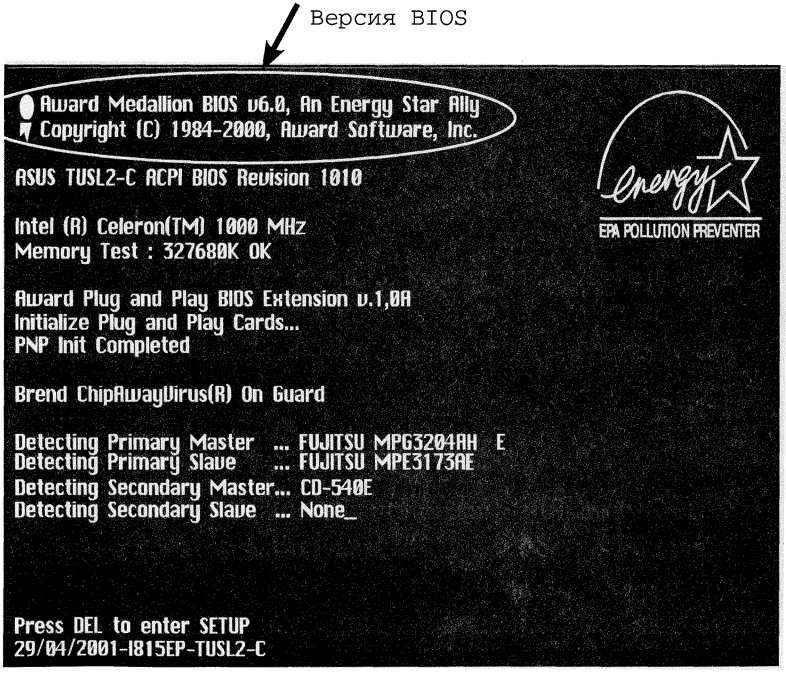


Рис. 11.1. Загрузка компьютера

водит самотестирование и выявляет проблемы с внутренними устройствами. Если проблемы есть, то он издает несколько гудков и прерывает загрузку. По идее, теперь вы должны нести свой компьютер в мастерскую или вызывать компьютерного мастера.

Однако, по тому, какие это гудки и сколько их, зачастую можно судить о сути проблемы. Правда, для этого вы должны выяснить, какая у вас стоит версия BIOS. Версию можно увидеть сразу же после включения компьютера до того, как начнет загружаться Windows. Если у вас вообще никакой информации не появляется на экране, то вам остается только попробовать подобрать один из подходящих вариантов.

Далее приведена расшифровка звуков, издаваемых компьютерами (в случае неполадок) в зависимости от версии BIOS.

11.2. Звуковые сигналы в AWARD BIOS

Сигналов нет (никаких)

Не поступает питание к материнской плате: блок питания не подключен к материнской плате или неисправен.

Непрерывный сигнал

Ошибка в блоке питания. Он требует замены.

Один короткий сигнал

Все прошло без ошибок.

Один короткий повторяющийся

Нестабильно работает блок питания. Ошибка может быть вызвана, например, скопившейся пылью.

Один длинный повторяющийся

Ошибка модулей оперативной памяти. Если перед этим производились какие-нибудь замены – возможно, модули неправильно установлены. Если перемен не было – скорее всего, один из блоков неисправен.

Один длинный + один короткий сигнал

Ошибка оперативной памяти. Возможно, модули неправильно установлены. Но, скорее всего, один из блоков неисправен.

Один длинный + два коротких сигнала

Ошибка видеокарты. Возможны варианты: неисправна собственная память видеокарты – видеопамять; плата плохо вставлена в слот материнской платы или же плохо соединена с монитором.

Один длинный + три коротких сигнала

Проблемы с инициализацией клавиатуры: необходимо проверить соединения клавиатуры и материнской платы.

Один длинный + девять коротких сигналов

Ошибка чтения из микросхемы постоянной памяти. Попробуйте загрузить компьютер снова, если не помогает, микросхему обычно заменяют или, если позволяет ее устройство, перезаписывают («перепрошивают»).

2 коротких сигнала

Обычно этот сигнал выдается при незначительных ошибках. Иногда – при неудачных попытках изменить настрой-

ки BIOS`а (неустойчивая работа устройств) или при плохих соединениях шлейфа с материнской платой или жестким диском. Исправляют настройки (устанавливают стабильные значения или откатывают к заводским) и проверяют соединения.

Три длинных сигнала

Ошибка материнской платы, связанная с контроллером клавиатуры. Проверьте соединения и попробуйте перезагрузиться.

11.3. Звуковые сигналы в AMI BIOS

Сигналов нет (никаких)

Не поступает питание к материнской плате: блок питания не подключен к материнской плате или неисправен.

1 короткий сигнал

Все прошло без ошибок.

2 коротких сигнала

Ошибка модулей оперативной памяти (проблема четности). Если перед этим производились какие-нибудь замены – возможно, модули неправильно установлены. Если перемен не было – скорее всего, один из блоков неисправен.

3 коротких сигнала

Ошибка оперативной памяти (первые 64 Кб). Возможно, модули неправильно установлены. Но, скорее всего, один из модулей неисправен.

4 КОРОТКИХ СИГНАЛА

Ошибка системного таймера материнской платы или модуля памяти в первом слоте. Если повторная перезагрузка пройдет с тем же результатом – придется менять материнскую плату.

5 КОРОТКИХ СИГНАЛОВ

Ошибка центрального процессора. Если повторная перезагрузка пройдет с тем же результатом – придется его менять.

6 КОРОТКИХ СИГНАЛОВ

Ошибка материнской платы, связанная с контроллером клавиатуры. Проверьте соединения и попробуйте перезагрузиться.

7 КОРОТКИХ СИГНАЛОВ

Общая ошибка материнской платы. Все проверьте и загрузитесь снова – попробуйте выяснить, что именно испортилось. Если не удается ничего уточнить – заменяйте материнскую плату.

8 КОРОТКИХ СИГНАЛОВ

Неисправна собственная память видеокарты – видеопамять. Необходимо заменить либо модули памяти, либо всю видеокарту.

9 коротких сигналов

Ошибка микросхемы постоянной памяти BIOS. Попробуйте загрузить компьютер снова, если не помогает, микросхему обычно заменяют или, если позволяет ее устройство, перезаписывают («перепрошивают»).

10 коротких сигналов

Ошибка записи в микросхеме CMOS-памяти. Попробуйте загрузить компьютер снова, если это не помогает, попробуйте сбросить содержимое CMOS-памяти. Иногда приходится заменять и материнскую плату.

11 коротких сигналов

Ошибка внешней кэш-памяти, установленной в спец. слотах материнской платы. Попробуйте загрузить компьютер снова, если это не помогает, замените микросхему кэш-памяти или выньте ее совсем.

1 длинный + 2 коротких сигнала, 1 длинный + 3 коротких сигнала

Ошибка видеокарты. Возможны варианты: неисправна собственная память видеокарты – видеопамять; плата плохо вставлена в слот материнской платы или же плохо соединена с монитором.

1 длинный + 8 коротких сигналов

Ошибка видеокарты. Может быть, плата плохо вставлена в слот материнской платы или же плохо соединена с монитором.

11.4. Звуковые сигналы в Phoenix BIOS

Нижеприведенные обозначения следует воспринимать следующим образом. Например, если написано `1-3-1`, то это значит, что сначала прозвучит один короткий сигнал, затем последует пауза, затем еще три коротких сигнала, затем снова пауза и в завершении еще один короткий сигнал. Достаточно редко, но встречаются сигналы из четырех групп, например `1-3-2-1`. О них можно почитать на сайте www.bioscentral.com (англ.).

1-1-3

Ошибка записи или чтения в микросхеме CMOS-памяти. Попробуйте загрузить компьютер снова, если не помогает, попробуйте сбросить содержимое CMOS-памяти. Проверьте также и работоспособность батарейки. Иногда приходится заменять и материнскую плату.

1-1-4

Ошибка микросхемы постоянной памяти (ошибка контрольной суммы), которая контролируется BIOS'ом и необходима для правильной загрузки. Попробуйте загрузить компьютер снова, если это не помогает, микросхему обычно заменяют или, если позволяет ее устройство, перезаписывают («перепрошивают»).

1-2-1

Общая ошибка материнской платы. Все проверьте и загрузитесь снова – попробуйте выяснить, что именно испортилось. Если не удается ничего уточнить – заменяйте материнскую плату.

1-2-2

Ошибка материнской платы (инициализация контроллера DMA). Все проверьте (попробуйте установить заводские значения BIOS) и загрузитесь снова. Если все безрезультатно – заменяйте материнскую плату.

1-2-3

Ошибка материнской платы (невозможно осуществить чтение/запись в один из каналов DMA). Все проверьте и загрузитесь снова. Если ничего не изменяется – заменяйте материнскую плату.

1-3-1

Ошибка оперативной памяти (проблема регенерации). Если перед этим производились какие-нибудь замены – возможно, модули неправильно установлены. Если замен не было – скорее всего, один из модулей неисправен.

1-3-3, 1-3-4

Ошибка оперативной памяти. Если перед этим производились какие-нибудь замены – возможно, модули неправильно установлены. Если замен не было – скорее всего, один из блоков неисправен.

1-4-1

Ошибка материнской платы (на адресной линии доступа к первым 64 Кб). Все проверьте и загрузитесь снова. Если ничего не изменяется – заменяйте материнскую плату.

1-4-2

Ошибка проверки оперативной памяти (ошибка тестирования). Если перед этим производились какие-нибудь замены – возможно, модули неправильно установлены. Проблема, скорее всего, в первом модуле оперативной памяти.

1-4-3

Ошибка системного таймера материнской платы. Если повторная перезагрузка пройдет с тем же результатом – придется менять материнскую плату.1-4-4

Ошибка порта ввода/вывода. Отключите подключенное к нему устройство – оно может быть причиной ошибки – и загрузитесь заново.

2-X-X

Все сигналы, начинающиеся с двух, извещают об ошибке доступа к оперативной памяти (первым 64 Кб).

3-1-1

Ошибка материнской платы (инициализация второго канала DMA). Все проверьте и загрузитесь снова. Если ничего не изменяется – заменяйте материнскую плату.

3-1-2

Ошибка материнской платы (инициализация первого канала DMA). Проверьте все соединения и загрузитесь снова. Попробуйте установить заводские значения опций в BIOS. Если ничего не изменяется – заменяйте материнскую плату.

3-1-4

Ошибка материнской платы (контроллер прерываний). Все проверьте (можно подождать некоторое время) и загрузитесь снова. Попробуйте установить заводские значения опций в BIOS. Если ничего не изменяется – заменяйте материнскую плату.

3-2-4

Проблемы с контроллером клавиатуры. Необходимо проверить соединения клавиатуры и материнской платы. При необходимости замените неисправные устройства (контроллер может быть выполнен в виде платы расширения).

3-3-4

Неисправна (ошибка тестирования) собственная память видеокарты – видеопамять. Необходимо заменить либо модули памяти, либо всю видеокарту (проверьте сначала, хорошо ли установлена видеокарта в своем слоте!).

4-2-1

Ошибка системного таймера материнской платы. Если повторная перезагрузка пройдет с тем же результатом – придется менять материнскую плату.

4-2-3

Проблемы с контроллером клавиатуры (адресной линии A20). При необходимости замените неисправные устройства (контроллер или материнскую плату).

4-2-4

Произошли ошибки в работе центрального процессора (ошибка защищенного режима). По возможности уточните «диагноз» еще как-нибудь.

4-3-1

Ошибка оперативной памяти (ошибка тестирования). Если перед этим производились какие-нибудь замены – возможно, модули неправильно установлены. Если перемен не было – скорее всего, один из блоков неисправен.

4-3-3

Ошибка системного таймера.

4-3-4

Ошибка материнской платы (неисправность в часах реального времени). Все проверьте и загрузитесь снова. Если ничего не изменяется – заменяйте материнскую плату.

4-4-1

Ошибка последовательного порта. Отключите подключенное к нему устройство – оно может быть причиной ошибки – и загрузитесь заново.

4-4-2

Ошибка параллельного порта. Отключите подключенное к нему устройство – оно может быть причиной ошибки – и загрузитесь заново.