Алексей Анатольевич Гладкий
Как защитить компьютер от ошибок, вирусов, хакеров

Введение

Ни для кого не является секретом тот факт, что в настоящее время компьютер прочно и надолго вошел в нашу повседневную жизнь. Его возможности используются на работе, при проведении досуга, в быту и других сферах жизнедеятельности человека. И с каждым днем растет количество информации, которая мы доверяем своему «электронному другу». Поэтому рано или поздно каждый пользователь задает себе вопрос – каким же образом можно обеспечить надежную сохранность своих данных?

В большинстве случаев такой вопрос возникает уже после того, как случилась определенная неприятность. Поэтому большинство пользователей принимает меры по обеспечению сохранности данных лишь после их полной либо частичной потери (либо при возникновении ситуации, когда потери данных удалось избежать только чудом). Для того чтобы не попадать в подобные переделки, достаточно соблюдать несложные правила безопасности.

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

Как известно, компьютерные технологии развиваются с каждым днем, и новые достижения могут использоваться не только во благо пользователей, но и, будучи применены со злым умыслом, способны причинить немалый ущерб. Поэтому, наряду с рекомендациями по избежанию потерь данных, в книге рассматриваются приемы и способы их восстановления, если подобная неприятность уже имела место.

Защищенность компьютера: мифы и реальность

Несмотря на то, что защищенность компьютера (а, следовательно – и хранящейся в нем информации) зависит от многих индивидуальных факторов (специфика его использования, загруженность, наличие опыта работы у пользователя и др.), имеется ряд общих причин, вызывающих потерю данных. С наиболее распространенными из них мы познакомимся в этой главе.

Однако перед этим не будет лишним вспомнить основные правила эксплуатации персонального компьютера, соблюдение которых не только продлевает срок его службы, но и имеет важное значение с точки зрения сохранности информации.

Основные правила эксплуатации компьютера

Основные правила эксплуатации компьютера придуманы не сегодня и не вчера; они формировались на основе многолетнего опыта использования компьютеров. Большинство пользователей наверняка знакомы с ними, но вот соблюдают их далеко не все. Эти правила перечислены ниже.

♦ По возможности минимизировать попадание пыли в системный блок. Пыль может вызывать перегрев компонентов компьютера, периодическое исчезновение контактов и др. Не рекомендуется устанавливать системный блок на пол, поскольку именно там обычно возникает наибольшее скопление пыли. Периодически (хотя бы раз в год) необходимо выполнять профилактическую уборку компьютера (удалять накопившуюся пыль с его компонентов).

♦ Следить за температурным режимом работы компонентов компьютера. Все установленные вентиляторы и кулеры должны функционировать, при поломке какого-либо из них необходимо оперативно его отремонтировать либо заменить. Для слежения за температурным режимом можно использовать специальные утилиты, множество которых можно найти в Интернете.

♦ Не следует устанавливать компьютер в местах, которые могут вызвать его преждевременный перегрев (например, в зоне попадания прямых солнечных лучей).

♦ Если компьютер какое-то время находился в холодном помещении либо на улице (с температурой ниже 0 градусов), то нужно дать ему постоять 2–3 часа в теплом помещении, и только после этого включать.

♦ Обеспечить нормальное электропитание. Качество отечественной электроэнергии оставляет желать много лучшего (об этом более подробно рассказывается ниже, в разделе «Проблемы с электропитанием»), поэтому необходимо защитить компьютер от возможных скачков напряжения, внезапного отключения электроэнергии и т. п. Как минимум, для этого необходимо использовать сетевой фильтр, а лучше всего – источник бесперебойного питания.

♦ Не стоит самостоятельно экспериментировать с внутренним устройством компьютера. Если необходимо внести какие-либо изменения в его конфигурацию, лучше доверить эту процедуру специалисту

(либо получить у него подробную консультацию). Например, несложная на первый взгляд операция – добавление оперативной памяти – может не только не привести к ожидаемым результатам (в частности, к увеличению быстродействия), но и вызвать неправильную работу некоторых приложений, что может закончиться большими неприятностями. А причина может быть в том, что выбранная «оперативка» просто несовместима с некоторым другим оборудованием, установленным на компьютере.

♦ Обязательно установить хорошую антивирусную программу. Даже если пользователь не выходит в Интернет, велик риск подхватить вирус с какой-либо дискеты, компакт-диска, из локальной сети и др. Периодически необходимо с помощью антивирусной программы выполнять полное сканирование компьютера на предмет обнаружения вирусов.

♦ При работе в Интернете настоятельно рекомендуется использовать брандмауэр либо файрвол. Стандартный интернет-обозреватель Internet Explorer имеет встроенный брандмауэр, однако опытные хакеры давно научились его обходить. Поэтому рекомендуется использовать другую защиту – например, все большую популярность завоевывает программа Zone Alarm. Она имеет как платную, так и бесплатную версии; каждую из них можно скачать в Интернете.

♦ Каждый сеанс работы должен завершаться корректно – с использованием штатной функциональности завершения работы операционной системы.

Причины потери информации

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

♦ нестабильная работа операционной системы;

♦ нестабильное электропитание (в т. ч. внезапное отключение электроэнергии);

♦ действия вирусов и других вредных программ;

♦ неквалифицированные действия пользователей (в частности, внесение некорректных изменений в системный реестр, безграмотное редактирование системных файлов, и т. п.);

♦ повреждение жесткого диска.

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

Нестабильная работа операционной системы

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

Подобная ситуация возникает, как правило, в результате того, что в процессе работы в операционной системе накапливаются различные вспомогательные файлы, библиотеки, настройки (например, в результате инсталляции программ) и т. п., которые со временем могут начать конфликтовать как друг с другом, так и с операционной системой. Ведь, несмотря на то, что большинство современных программ имеют встроенные режимы деинсталляции, не всегда удаление программы происходит корректно и бесследно для операционной системы (что уж говорить о приложениях, которые не имеют штатных средств для деинсталляции). Такие «хвосты» не только засоряют системный реестр, но и могут дополнительно отвлекать ресурсы оперативной памяти.

Чтобы избежать подобных неприятностей, рекомендуется периодически проводить чистку системного реестра. Разумеется, это делается не вручную – для чистки реестра следует применять специально разработанные программы и утилиты, которых в настоящее время имеется великое множество. Они могут быть платными, условно-платными и бесплатными; в качестве разработчиков выступает как корпорация Microsoft, так и целый ряд сторонних авторов. Дистрибутив либо исполняемый файл большинства таких программ можно легко найти в Интернете. В этой книге мы рассмотрим одну из популярных программ, которую удобно использовать для чистки реестра – менеджер реестра Reg Organizer, одним из достоинств которой является то, что она распространяется бесплатно.

Сразу отметим, что менеджер реестра Reg Organizer представляет собой многофункциональную утилиту, предназначенную для выполнения различных работ с системным реестром. В этой книге мы не будем подробно рассматривать все ее функциональные возможности, а остановимся лишь на тех из них, которые имеют непосредственное отношение к рассматриваемой проблеме.

Чистка системного реестра

Интерфейс программы в режиме чистки реестра представлен на рис. 1.1.

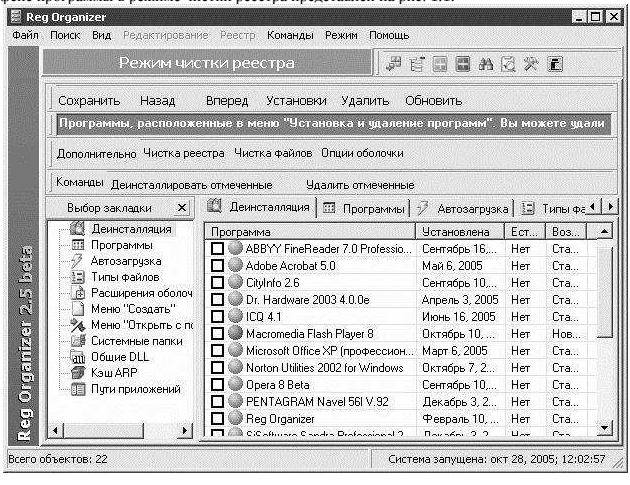


Рис. 1.1. Менеджер реестра Reg Organizer

Вообще в программе Reg Organizer предусмотрено использование нескольких режимов, перечень которых приводится ниже.

- ♦ Режим редактирования реестра.
- ♦ Режим чистки реестра.
- ♦ Режим редактирования файлов.
- ♦ Режим поиска и замены в реестре.
- ♦ Режим деинсталляции программ.

Выбор требуемого режима осуществляется с помощью соответствующей команды меню Режим (это меню включено в состав главного меню программы). Интерфейс, изображенный на рис. 1.1, откроется после выполнения команды Режим►Режим чистки реестра.

Перед тем, как приступить к чистке реестра, рекомендуется просмотреть и, при необходимости – отредактировать некоторые параметры работы программы. Для этого следует в инструментальной панели нажать кнопку Установки (см. рис. 1.1), и в открывшемся окне перейти на вкладку Поиск ссылок на несуществующие файлы. Здесь определяются разделы реестра, которые будут просканированы, порядок удаления неверных записей, и др. Порядок настройки параметров на данной вкладке прост и интуитивно понятен, поэтому подробно останавливаться на этом не будем.

Для того чтобы приступить к чистке реестра, следует нажать кнопку Чистка реестра (см. рис. 1.1). В результате на экране откроется окно, изображенное на рис. 1.2.

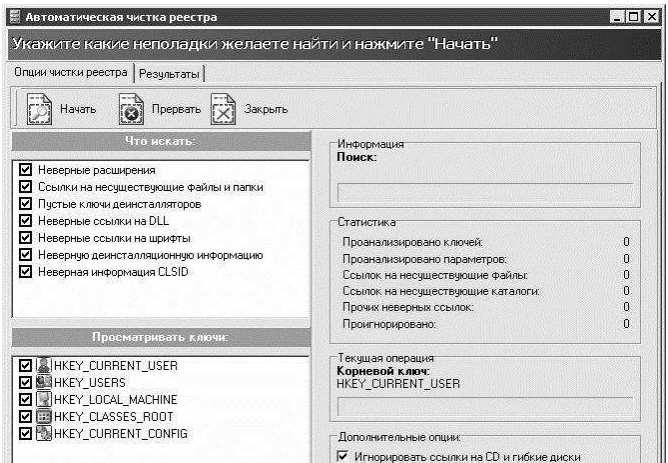


Рис. 1.2. Чистка реестра

В данном окне в поле Что искать определяются объекты поиска. Для выбора объектов предназначены флажки, перечень которых приведен ниже.

- ♦ Неверные расширения.
- ♦ Ссылки на несуществующие файлы и папки.
- ♦ Пустые ключи деинсталляторов.
- ♦ Неверные ссылки на DLL.
- ♦ Неверные ссылки на шрифты.
- ♦ Неверную деинсталляционную информацию.
- ♦ Неверная информация CLSID.

В поле Просматривать ключи аналогичным образом выбираются ключи реестра, которые должны быть просканированы. Следует учитывать, что выбор ключей возможен только в том случае, если в поле Что искать установлен флажок Ссылки на несуществующие файлы и папки (иначе говоря, выбор ключей имеет значение только для режима Ссылки на несуществующие файлы и папки). По умолчанию флажки установлены напротив тех ключей, которые выбраны в окне настройки параметров программы на вкладке Поиск ссылок на несуществующие файлы.

Справа внизу окна в группе флажков Дополнительные опции можно при необходимости установить дополнительные параметры сканирования. Для этого предназначены перечисленные ниже флажки.

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

Запуск процесса сканирования реестра осуществляется нажатием кнопки Начать, которая расположена в верхней части окна в инструментальной панели.

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

Чтобы остановить сканирование, нужно воспользоваться кнопкой Прервать. С помощью кнопки

Закрыть осуществляется выход из данного режима.

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

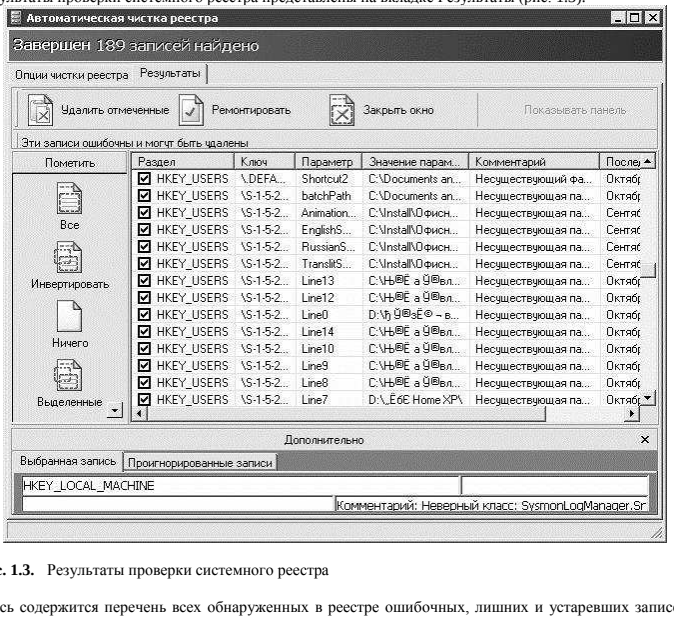


Рис. 1.3. Результаты проверки системного реестра

Здесь содержится перечень всех обнаруженных в реестре ошибочных, лишних и устаревших записей, которые могут быть удалены. Для каждой позиции списка в соответствующих колонках отображается раздел, ключ и параметр реестра, значение параметра, комментарий (иначе говоря – тип записи) и дата последнего изменения.

С помощью кнопки Ремонтировать, которая расположена в инструментальной панели (рис. 1.3), можно перейти в режим поиска объектов, на которые указывают неверные ссылки. Однако использование этой возможности позволяет исправить только ссылки на несуществующие файлы (в значениях параметров) и неверные ссылки на шрифты; прочие виды ссылок будут проигнорированы.

По умолчанию все позиции списка помечены с помощью флажков, установленных слева от каждой позиции. При нажатии кнопки Удалить отмеченные, которая также находится в инструментальной панели, из системного реестра будут удалены все отмеченные в списке записи. При необходимости можно выполнить выборочное удаление ошибочных записей из реестра.

В левой части интерфейса расположена панель Пометить. В ней находится несколько кнопок. С помощью кнопки Все осуществляется быстрая пометка одновременно всех позиций списка. Кнопка Инвертировать предназначена для пометки/снятия пометок одновременно со всех позиций списка. При нажатии кнопки Ничего будут сняты пометки со всех позиций списка. Кнопка Выделенные используется для пометки позиций списка, которые выделены курсором.

Если, находясь на любой позиции списка, нажать правую кнопку мыши, то откроется контекстное меню, содержащее перечисленные ниже команды.

♦ Открыть ключ в редакторе реестра – при активизации данной команды выделенная курсором позиция списка будет открыта в режиме редактирования реестра.

♦ Добавить элемент в список исключений – с помощью данной команды осуществляется добавление текущей позиции списка в список исключений.

ПРИМЕЧАНИЕ

В программе Reg Organizer реализована возможность ведения списка исключений. Записи, добавленные в данный список, при последующих проверках системного реестра за ошибку не принимаются.

♦ Добавить все выбранные элементы в список исключений – при выполнении этой команды в список исключения будут добавлены все отмеченные позиции.

♦ Список исключений – команда предназначена для перехода в режим работы со списком исключений.

♦ Сохранить список как – эта команда используется для сохранения списка ошибочных записей в отдельном текстовом файле. Данную возможность целесообразно использовать, например, в случае, когда необходимо подробно проанализировать содержимое списка, но в данный момент по каким-то причинам это невозможно. При выполнении команды на экране открывается окно Сохранить как, в котором по обычным правилам Windows указывается путь для сохранения и имя файла.

Перед удалением отмеченных записей из реестра Reg Organizer по умолчанию автоматически создает резервную копию удаленных данных. Для работы с резервными копиями (восстановление, удаление и т. п.) предназначена команда главного меню программы Команды►Резервные копии.

Чистка файлов

Помимо чистки системного реестра, программа Reg Organizer позволяет выполнять файловую чистку системы. Для перехода в соответствующий режим нужно в окне, изображенном на рис. 1.1, нажать кнопку Чистка файлов – в результате на экране откроется окно, которое показано на рис. 1.4.

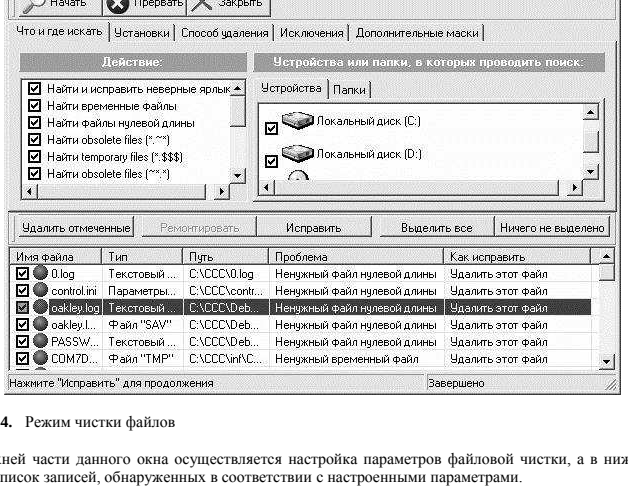


Рис. 1.4. Режим чистки файлов

В верхней части данного окна осуществляется настройка параметров файловой чистки, а в нижней – выводится список записей, обнаруженных в соответствии с настроенными параметрами.

Верхняя часть окна состоит из нескольких вкладок. Кратко остановимся на каждой из них.

На вкладке Что и где искать в поле Действие путем установки соответствующих флажков выбираются типы объектов, которые нужно найти (временные файлы, файлы нулевой длины и т. п.). В расположенном правее поле Устройства или папки, в которых производить поиск определяются диски и папки компьютера, в которых будет произведен поиск (диски выбираются с помощью соответствующих флажков на вкладке Устройства, список папок формируется на вкладке Папки).

На вкладке Установки выполняется настройка процесса сканирования. Для этого предназначены флажки, перечень которых приведен ниже.

♦ Игнорировать ссылки на CD-ROM.

♦ Игнорировать ссылки на гибкие и иные отсоединяемые диски.

♦ Игнорировать ссылки на сетевые и RAM-диски.

♦ Пропускать системные файлы и папки (этот флажок настоятельно рекомендуется установить).

♦ Пропускать скрытые файлы и папки.

По умолчанию установлены все флажки, кроме флажка Пропускать скрытые файлы и папки.

На вкладке Способ удаления определяется, каким образом должно выполняться удаление найденных объектов. Возможные варианты:

♦ Стирать с диска;

♦ Удалять в Корзину;

♦ Перемещать в папку (при выборе данного варианта следует указать путь к папке, в которую должны быть помещены найденные объекты при удалении).

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

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

Запуск процесса сканирования в соответствии с настроенными параметрами осуществляется нажатием кнопки Начать, которая расположена в инструментальной панели интерфейса. Если необходимо остановить поиск, то нужно нажать расположенную правее кнопку Прервать.

По окончании сканирования список найденных файлов выводится в нижней части окна (рис. 1.4). Для каждой позиции списка в соответствующих колонках показывается следующая информация:

♦ имя найденного файла;

♦ тип файла (текстовый, временный и т. п.);

♦ полный путь к файлу;

♦ краткое описание проблемы (почему файл считается ненужным);

♦ рекомендуемый способ исправления, а после исправления – состояние (статус) файла (например, Удален).

Чтобы удалить файлы из списка, нужно предварительно пометить их с помощью флажков, устанавливаемых слева от имени файла, и нажать кнопку Удалить отмеченные. Для быстрой пометки всех позиций списка предназначена кнопка Выделить все, для снятия пометок со всех позиций следует воспользоваться кнопкой Ничего не выделено. С помощью кнопки Исправить осуществляется исправление всех записей в соответствии со способом, рекомендованным в колонке Как исправить.

С помощью рассмотренной функциональности можно быстро очистить систему от ненужных и неиспользуемых файлов.

Проблемы с электропитанием

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

Дело в том, что персональный компьютер представляет собой гораздо более тонкий механизм, чем остальная техника. И перепады напряжения в электрической сети, не имеющие никаких последствий, например, для холодильника или телевизора, могут в то же время привести к серьезной поломке компьютера. Причины перепадов напряжения могут быть самые разные – от природных катаклизмов (например, гроза) до внезапно включенной соседом электродрели (да и без этого, как отмечалось выше, отечественная электроэнергия может преподнести неприятный сюрприз).

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

Кроме этого, можно отметить еще одну неприятную особенность, которая также проявляется в основном в домах советской постройки. Электрические сети, проложенные в таких домах, не рассчитаны на современную нагрузку – ведь в то время у людей не было такого количества бытовой техники, как сейчас. Если раньше в стандартном доме было, может, три-пять стиральных машин на подъезд, то сейчас они есть почти в каждой квартире; раньше нормой считался один телевизор в квартире, а сейчас многие имеют по два (а то и три) телевизора. Плюс к этому, многие сегодня имеют различного рода электрочайники-обогреватели-микроволновки и т. д. Это какая же нагрузка ложится на сеть, проложенную в 60-х – 80-х годах! Поэтому многим известна примерно такая ситуация – сосед включил электрочайник (или

обогреватель), и по всему «стояку» в подъезде отключился свет.

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

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

В первую очередь отметим, что ни в коем случае нельзя включать компьютер (а также – монитор) в обычную электрическую розетку – это верный способ быстро вывести его из строя. Как минимум, необходимо использовать сетевой фильтр – иногда он продается в комплекте с компьютером, но чаще его приходится приобретать отдельно. Сетевой фильтр внешне представляет собой обычный «тройник»-удлинитель (только гнезд в нем не три, а четыре или пять), снабженный тумблером-выключателем. Однако такой фильтр способен защитить компьютер только от несущественных перепадов напряжения, и совершенно бесполезен при внезапном отключении электроэнергии.

Для более надежной защиты компьютера от сбоев с электропитанием рекомендуется использовать специальный прибор – источник бесперебойного питания. Его характерной особенностью является то, что компьютер питается именно от него, а не непосредственно из сети. Иначе говоря, источник бесперебойного питания – это своеобразный буфер между электрической сетью и компьютером. В его состав, помимо прочего, входит аккумуляторная батарея (перед первым использованием ее нужно заряжать примерно 4–6 часов; подробно об этом рассказывается в руководстве пользователя), средний срок службы которой – от трех до пяти лет. Эта батарея позволяет корректно завершить работу компьютера и спокойно выключить его даже после внезапного отключения электроэнергии.

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

В настоящее время на рынке представлено множество различных источников бесперебойного питания – как отечественного производства, так и импортных. При выборе следует руководствоваться в первую очередь его техническими характеристиками, а именно – подходит ли он к конкретному компьютеру. Не рекомендуется приобретать источник бесперебойного питания с рук либо на рынке.

Действия вирусов и других вредных программ

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

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

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

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

Неквалифицированные действия пользователей

Наверное, ни один вирус и никакой перепад напряжения в сети не могут причинить такого ущерба

компьютеру и хранящейся в нем информации, который могут вызвать неквалифицированные действия пользователя. Такие действия можно условно разделить на три группы:

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

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

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

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

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

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

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

> **ВНИМАНИЕ**
>
> В большинстве современных файловых менеджеров (Total Commander, Far и др.) имеется режим отображения информации, при использовании которого системные и загрузочные файлы не показываются. Настоятельно рекомендуется включить этот режим, чтобы не было соблазнов поредактировать такие файлы (разумеется, если пользователь дорожит информацией, хранящейся в компьютере).

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

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

Повреждение жесткого диска

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

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

ПРИМЕЧАНИЕ

В большинстве случаев с поврежденного жесткого диска можно восстановить только небольшие файлы, размер которых находится в пределах 150 Кб.

Подробно рассматривать способы восстановления информации с поврежденного жесткого диска здесь мы не будем, поскольку об этом рассказывается ниже, в соответствующем разделе.

Отметим, что для восстановления данных можно также обратиться к специалистам. Однако при этом следует учитывать, что скорее всего полностью восстановить данные все равно не удастся, а финансовые затраты наверняка будут достаточно велики.

Уязвимые места компьютера

Несмотря на то, что при грамотном использовании компьютера его надежность намного повышается, в любом случае у него имеются свои уязвимые места, которым нужно уделять особое внимание. Некоторые из них находятся в аппаратной части компьютера, остальные (которых большинство) – в программной его части. Далее мы рассмотрим и те, и другие более подробно.

Аппаратная часть компьютера

Каким же компоненты аппаратной части компьютера наиболее подвержены поломкам?

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

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

Однако необходимо учитывать, что BIOS может и не сообщить о неполадках с «железом». Например, автор лично столкнулся с такой ситуацией: операционная система не загружается по непонятным причинам, при этом BIOS выдает один короткий сигнал, что означает – с аппаратной частью все в порядке. Попытки переустановить систему с загрузочного компакт-диска также ни к чему не привели – переустановка прекращалась уже на начальном этапе (компьютер «зависал»). В данном случае помогло знание уязвимых мест собственного компьютера: пришлось просто достать оперативную память, протереть тряпочкой и вновь поставить ее на место – после этого все проблемы исчезли, операционная система вновь стала загружаться, даже переустанавливать ее не пришлось. Вывод – несмотря на общие закономерности, каждый компьютер имеет свои индивидуальные уязвимые места, и если пользователь знает о них, то это избавит его от многих дополнительных проблем.

Как отмечалось выше, к уязвимым компонентам аппаратной части компьютера можно отнести монитор. Несмотря на то, что в настоящее время на отечественном рынке представлен широкий ассортимент высококачественных мониторов, нередко они выходят из строя, не отработав даже гарантийного срока службы. Проблема здесь не в качестве мониторов, а в качестве используемых электрических сетей (как

отмечалось выше, подавляющее большинство электросетей на территории СНГ не имеют заземления). Чтобы минимизировать вероятность поломки монитора, рекомендуется обязательно отключать его от сети по окончании работы (некоторые пользователи не выключают монитор сутки напролет, независимо от того, работают они или нет), а также избегать различного рода автоматических переключений режимов (переход в экономный режим после простоя в течение определенного промежутка времени и т. п.) – при отсутствии заземления это повышает риск выхода монитора из строя. Кстати, по этой же причине не рекомендуется слишком часто использовать различного рода ждущие/спящие режимы работы компьютера – повышается вероятность выхода из строя того или иного оборудования.

Если полностью выходит из строя блок питания, то компьютер включить не удастся. Однако в большинстве случаев блок питания выходит из строя не моментально. Перед этим пользователь замечает признаки нестабильности в работе – в частности, компьютер может произвольно перезагружаться. При появлении подобных симптомов следует немедленно выяснить, чем они вызваны – это может быть как неисправность блока питания (в первую очередь нужно проверить, не перегревается ли он), так и проблемы с жестким диском. В последнем случае возможно проявление дополнительных симптомов: заметное падение быстродействия работы компьютера, увеличение шума, издаваемого жестким диском, возникновение ошибок при чтении файлов. Если имеет место хотя бы один из этих признаков, то следует немедленно позаботиться о сохранении всех важных данных на внешнем носителе информации – в противном случае велик риск их безвозвратной потери.

Материнская плата – один из важнейших компонентов персонального компьютера. Она координирует и сводит воедино работу других механизмов и компонентов. Если выходит из строя материнская плата, то возможные последствия зависят от характера поломки. При частичных поломках нередко сохраняется возможность продолжения работы – это касается, например, выхода из строя некоторых портов. Если же материнская плата полностью выходит из строя (например, перегорела в результате перепадов напряжения), то работа на компьютере становится невозможной. Настоятельно рекомендуется при возникновении подозрений о частичном выходе из строя материнской платы провести диагностику и устранить неисправности (вплоть до замены материнской платы), так как в некоторых случаях частичный выход из строя материнской платы может привести к поломкам и другого оборудования – в частности, процессора и оперативной памяти.

Программная часть компьютера

Как отмечалось выше, большинство уязвимых мест компьютера содержится в его программной части. Их возникновение обусловлено целым рядом факторов: неквалифицированные либо ошибочные действия пользователя, конфликтные ситуации, возникающие между разными приложениями либо приложением и операционной системой, нестабильная работа операционной системы, программные ошибки (от которых не застраховано ни одно приложение), действия вредоносных программ (вирусов, троянов и т. п.) и др.

Какие же программные места компьютера наиболее уязвимы?

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

Кроме этого, в системном реестре регистрируются многие устанавливаемые на компьютер приложения. Поэтому при удалении программ с компьютера следует не просто удалить соответствующую папку из каталога Program Files (или другого места, где установлена программа), а воспользоваться специально предназначенной функциональностью, вызов которой осуществляется с помощью команды Пуск►Панель управления►Установка и удаление программ. Хотя даже в этом случае не все программы полностью удаляют следы своего пребывания на компьютере. Со временем подобные «хвосты» накапливаются в реестре, что никак не способствует стабильной работе системы (о том, как бороться с нестабильностью операционной системы, рассказано выше, в разделе «Нестабильная работа системы»).

Немалый ущерб системному реестру могут причинить различного рода вирусы. О разновидностях вирусов и о том, как с ними бороться, рассказывается ниже, в соответствующей главе.

Вообще следует отметить, что операционные системы семейства Windows достаточно уязвимы. Но это связано в первую очередь не с какими-то их конструктивными недостатками, а с тем, что ввиду широкой распространенности они хорошо изучены хакерами, взломщиками и т. п. «деятелями». Поэтому корпорация Microsoft вынуждена периодически выпускать различного рода «заплатки» для повышения защищенности системы.

Операционные системы UNIX и Linux с точки зрения защищенности выглядят более предпочтительно

(в первую очередь потому, что они не так досконально изучены распространителями вредоносных программ). Однако в настоящее время они не получили такого широкого распространения, как системы семейства Windows.

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

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

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

Вирусы и антивирусы

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

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

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

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

В конечном итоге вирусы стали создаваться с конкретными целями. Например, сотрудник, вынужденный уволиться с работы и считающий себя обиженным, с помощью вируса мог «отомстить» своему бывшему работодателю либо коллегам по работе. Кстати, подобные ситуации возникали и в корпорации Microsoft – известны случаи, когда бывшие ее сотрудники создавали вирусы, используя свои знания уязвимых мест операционной системы Windows либо офисных приложений.

В настоящее время в мире развелось великое множество «вирусописателей». Одни из них занимаются созданием и распространением вирусов в качестве хобби, другие просто желают сделать «всем плохо», третьи сводят с кем-то счеты, четвертые имеют вполне конкретные коммерческие цели – хищение

информации либо денежных средств, вывод из строя сетей, веб-ресурсов и т. п. за солидное вознаграждение (в частности, это одно из проявлений современной конкурентной борьбы), и др.

Все известные вирусы можно классифицировать по ряду признаков. Этим мы займемся в следующем разделе.

Разновидности вирусов

В настоящее время не существует единой классификации известных вирусов – многие специалисты расходятся во мнениях в данном вопросе. Одни предлагают в качестве признака классификации использовать среду обитания вируса, другие – его разрушительные способности, третьи – способ распространения, и др. Мы же классифицируем вирусы по наиболее характерным признакам.

В общем случае известные вирусы можно разделить на следующие группы:

- ♦ файловые вирусы;
- ♦ сетевые вирусы (черви);
- ♦ загрузочные вирусы;
- ♦ макровирусы;
- ♦ трояны.

Рассмотрим подробнее каждый из перечисленных видов.

Пик распространения файловых вирусов пришелся на конец 80-х – начало 90-х годов прошлого столетия. Их отличительной чертой является то, что они инициируются при запуске зараженной программы. Код вируса скрывается либо в исполняемом файле этой программы (файл с расширением exe или bat), либо в какой-нибудь из используемых программой динамических библиотек (dll). После активизации файловый вирус способен инфицировать другие программы, установленные на компьютере.

Следует, однако, отметить, что время файловых вирусов заканчивается. Исключение составляют только те из них, которые представляют собой скрипты. Такие вирусы, как правило, входят в состав веб-страниц и написаны с использованием скриптового языка программирования (например, JavaScript).

Основное место «проживания» и функционирования сетевых вирусов (червей) – локальная сеть. Обычно сетевой вирус, попадая на компьютер, самостоятельно распространяется по остальным компьютерам, входящим в состав сети. Некоторые сетевые вирусы могут использовать своеобразную «приманку» для того, чтобы пользователь инициировал их выполнение. Например, на рабочем столе зараженного компьютера может внезапно появится иконка с текстом вроде Нажми меня или Срочное сообщение; после щелчка мышью на такой иконке вирус будет активизирован.

Характерной особенностью загрузочных вирусов является то, что они поражают загрузочную область диска (как жесткого, так и гибкого). Действует такой вирус следующим образом: при загрузке компьютера данные из зараженной загрузочной области поступают в память компьютера. После этого инфицируются загрузочные области всех имеющихся жестких дисков, а также доступных гибких дисков. В настоящее время загрузочные вирусы слабо распространены, поскольку основной способ их размножения – через загрузочные гибкие диски, а сегодня мало кто пользуется загрузкой с гибкого диска.

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

Широкое распространение в настоящее время получили так называемые «троянские кони», либо, как их сокращенно называют – трояны. Их отличительной особенностью является то, что они, как правило, не причиняют ущерб компьютеру либо хранящейся в нем информации. Основное функциональное назначение троянов – предоставить к данному компьютеру свободный доступ через Интернет с удаленного компьютера. А уже этот удаленный пользователь может делать с зараженным компьютером все, что угодно – удалять и записывать информацию, редактировать параметры настройки, запускать программы и т. д. Цели при этом могут преследоваться совершенно разные – кража конфиденциальной информации, взлом паролей, рассылка спама и др. Причем, если с зараженного компьютера осуществляется, например, рассылка спама, то всю ответственность за это будет нести ничего не подозревающий владелец этого компьютера, а не удаленный

пользователь, реально управляющий данным процессом. В этом и заключается основное коварство троянов – пользователь зараженного компьютера не подозревает о том, что его компьютер используется посторонними лицами (причем нередко – в противозаконных целях). Для эффективной защиты от троянов недостаточно использовать только антивирусную программу – нужно еще установить на компьютер брандмауэр (файрвол); подробнее о таких защитных программах рассказывается ниже, в главе «Чем опасен Интернет».

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

Лучшие антивирусные программы

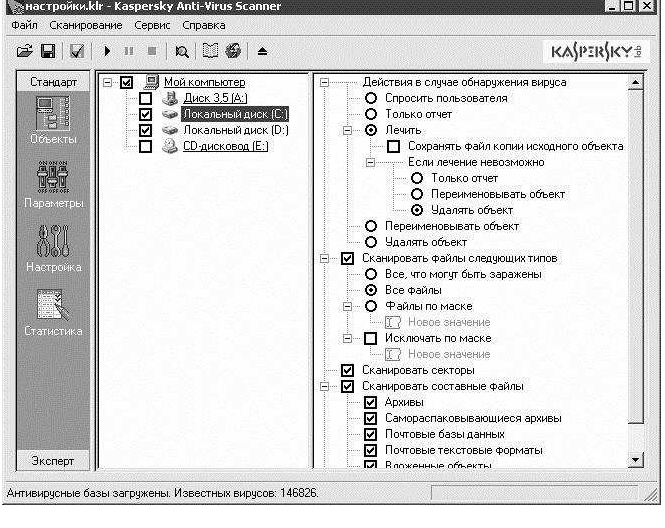
Как отмечалось выше, в настоящее время в Интернете существует великое множество разнообразных вирусов. Поэтому любой современный компьютер должен иметь установленную антивирусную программу. В настоящее время на отечественном рынке представлено достаточное количество различных антивирусных программ. В этой книге мы приведем обзор наиболее популярных из них.

В настоящее время на отечественном рынке представлено множество самых разнообразных антивирусных программ. Некоторые из них распространяются бесплатно, некоторые – на платной основе. Следует отметить, что эффективность платных антивирусных программ существенно выше, чем бесплатных. Поэтому для надежной защиты компьютера (особенно при частом использовании Интернета, а также при работе в локальной сети) рекомендуется устанавливать платные программы.

Признанными лидерами антивирусных программ в настоящее время являются программы Kaspersky Anti-Virus, Dr.Web и Norton Antivirus; все они являются платными.

Программа Kaspersky Anti-Virus

Программа Kaspersky Anti-Virus разрабатывается и сопровождается известной лабораторией Касперского. Первый образец антивируса вышел в свет еще в 1994 году. Конечно, в то время это был продукт, мало напоминающий мощную современную программу Kaspersky Anti-Virus. В настоящее время пользователь, приобретающий Kaspersky Anti-Virus, получает сразу несколько разных модулей: Kaspersky Anti-Virus Scanner, Kaspersky Anti-Virus Monitor, Kaspersky Anti-Virus Mail Checker, Kaspersky Anti-Virus Script Checker, Kaspersky Anti-Virus Updater и др., в зависимости от приобретаемого пакета.



Модуль Kaspersky Anti-Virus Scanner предназначен для сканирования компьютера (либо указанных объектов) на предмет заражения вирусами. Для вызова этого модуля можно использовать ярлык на рабочем столе либо соответствующую команду, которая после установки программы появится в меню кнопки Пуск. Также Kaspersky Anti-Virus Scanner будет доступен в контекстном меню, которое вызывается нажатием правой кнопки мыши в окне Проводника при выделении курсором какой-либо папки или файла. Это очень удобно, когда необходимо быстро просканировать какой-либо объект, поскольку избавляет пользователя от необходимости вызывать интерфейс программы и указывать в настройках сканируемый объект.

С помощью модуля Kaspersky Anti-Virus Monitor осуществляется постоянный мониторинг за состоянием компьютера и приложений. Данный режим настоятельно рекомендуется использовать при работе в Интернете. При обнаружении вирусов Kaspersky Anti-Virus Monitor тут же сигнализирует об этом путем вывода на экран соответствующего информационного окна. Следует отметить, что при включенном Kaspersky Anti-Virus Monitor снижается скорость работы системы.