**ТЕМА: РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ. ВОСТАНОВЛЕНИЕ ДАННЫХ.**

**Методы и средства обеспечения целост­ности данных**

Защита данных (к которым можно отнести и установленное программное обес­печение) от удаления или искажения задача непростая даже при отсутствии преднамеренных действий со стороны злоумышленников. Как правило, для ее решения требуется использовать комплекс программно технических мер, ос­новными из которых являются:

* резервное копирование данных;
* продуманная настройка и поддержание требуемых («безопасных») зна­чений системных параметров;
* заблаговременная установка и освоение специализированных про­граммных средств восстановления данных.

Перечисленные меры должны быть предусмотрены на этапе разработки поли­тики безопасности организации и отражены в соответствующих регламенти­рующих документах (в документе о политике безопасности, в частных инст­рукциях структурных подразделений и в должностных обязанностях исполни­телей).

***Резервное копирование данных***

Резервное копирование можно считать панацеей практически во всех ситуаци­ях, связанных с потерей или искажением данных. Одна­ко действительно универсальным «лекарством» резервное копирование ока­жется лишь в том случае, если соблюдать правила его применения. Особенности восстановления различных видов данных на основе резервных копий *будут приведены в соответствующих главах раздела сейчас*рассмотрим общие принципы резервного копирования.

**Архивация и резервное копирование**

Два этих понятия так часто используются совместно и публикациях и при ра­боте с данными, что иногда даже начинают восприниматься как синонимы. На самом деле, хотя архивация (английский термин archiving) и резервное копирование (backup) - большие «друзья», они вовсе не близнецы и вообще не «родственники».

что стоит за каждым из этих терминов?

**Архивация**очень близка к созданию некомпьютерных, «бумаж­ных» архивов. Архив - это место, приспособленное для хранения документов, которые либо потеряли свою актуальность, ли­бо используются относительно редко.

Документы в архиве обычно упорядочены (но датам, по логике, по авторству и т. д.). Это позволяет быстрoотыскать интересующий документ, корректно добавить новый документ или удалить не­нужный.

Практически все перечисленные особенности присущи также электронным ар­хивам. Причем ведущую роль при их создании играет умение программ-архиваторов сжимать архивируемые данные, позволяя тем самым экономить место для их хранения. Именно эта способность архиваторов и «подружила» их с программами резервного копирования, но подробнее об этом немного поз­же.

Цель **резервного копирования**на компьютере - повысить надежность хране­ния тех данных, потеря которых может огорчить (мягко говоря) их владельца. Для особо ценных данных могут создаваться две и более резервных копии. Как правило, при резервном копировании приходится решать две взаимосвя­занные проблемы: какие именно данные копировать, и как часто. С одной сто­роны, чем чаще выполняется копирование, тем меньше придется тратить сил на восстановление документа, потерянного, например, из-за отказа жестко­го диска. С другой стороны, создание каждой новой копии требует затрат вре­мени и места для ее хранения. Во многих случаях именно применение мето­дов сжатия, реализованных в программах-архиваторах, позволяет подобрать подходящие параметры процедуры резервного копирования. Существеннымотличием резервного копирования от архивацииявляется то, что хотя бы одна резервная копия обязательно должна быть создана не на же­стком диске, хранящем оригинал, а на альтернативном носителе (ком­пакт-диске и т. д.).

Еще одно различие между архивацией и резервным копированиемприведе­но далее.

Вы можете создать архив, включив в него редко используемые данные, и со­хранить его либо непосредственно на жестком диске компьютера, либо (что предпочтительнее, но не обязательно) на другом носителе. И после этогоуда­лить исходные файлы (оригиналы).

Процедура резервного копирования предполагает обязательное сохранение оригинала(то есть тех данных, с которыми работает пользователь). Резервное копирование предназначено в первую очередь для повышениясо­хранности данных, которые продолжают использоватьсяв работе (то есть пе­риодически изменяются). Поэтомурезервные копии также должны периодиче­ски обновляться. При этом обязательным является применение дополнитель­ных носителей данных (запоминающих устройств). В идеале для хранения ка­ждой копии следует отвести отдельный носитель.

**Методы резервного копирования**

Резервное копирование обычно осуществляется в соответствии с одним из трех основных методов: ***полным, инкрементальным и дифференциальным***.

При использовании **полного резервирования**каждый раз производится копи­рование всего набора данных. Например, копируется целиком файловая систе­ма, база данных или указанный каталог на диске. Данный метод занимает мно­го времени при записи и ведет к большому расходу резервных носителей. С другой стороны, в этом случае восстановление информации осуществляется быстрее, чем при любом другом методе, поскольку резервная копия соответст­вует текущему состоянию всего набора данных (с учетом периодичности копи­рования). Полное копирование является наиболее привлекательным решением при резервном копировании системной информации и служит отправной точ­кой для других методов

**Инкрементальный**(или добавочный) метод основан на последовательном частичном обновлении резервной копии. Напервом этапесоздается полная ко­пия набора данных. Последующие сеансы резервного копирования разделяют­ся на два вида: частичное копирование и полное. Приочередном частичномкопировании на резервный носитель помещаются только файлы, которые были  
модифицированы по сравнению с предыдущей частичной копией (на рис. схематично показана процедура инкрементального резервного копирования для недельного цикла). Модифицированными считаютсяфайлы, у которых из­менились содержание, атрибуты или права доступа. По истечении периода времени, заданного пользователем (или системным администратором)вновь создается полная копия, и затем цикл повторяется. Данный метод является са­мым быстрым сточки зрения создания промежуточных копий и ведет к минимальному расходу резервных носителей.

Однако процедура восстанов­ления занимает много времени: информацию сначала требуется восстановить с полной копии, а затем последовательно со всех частичных (инкременталь­ных) копий. Тем не менее, это самый популярный метод резервного копирования.

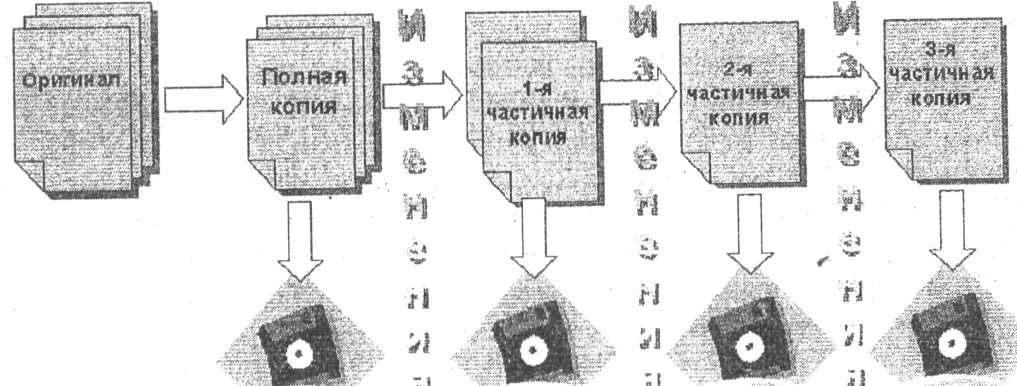


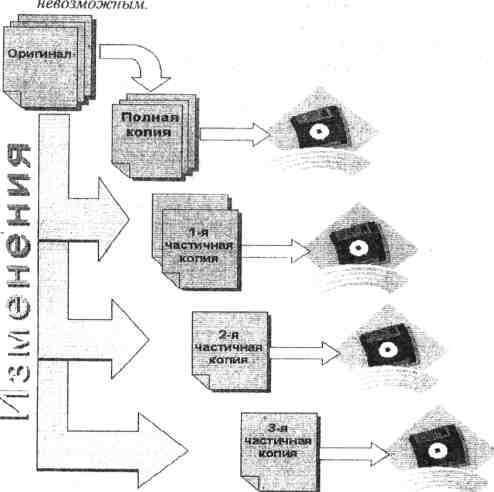
Рис. Схема инкрементального резервного копирования для недельного цикла

При **дифференциальном**(разностном) методе на первом этапе такжесоздается полная копия. На последующих этапах копируются только файлы, измененные со времени проведения полного копирования (на рис. приведена схема дифференциального резервного копирования для недельного цикла). Через за­данный интервал времени возобновляется полный цикл, то есть вновь создает­ся полная резервная копия набора данных. По сравнению с инкрементальным методом, дифференциальное копирование требует больше времени на создание частичной (дифференциальной) копии, но восстановление информации выпол­няется быстрее, поскольку используются только две копии: полная и последняя дифференциальная.

Главной проблемой инкрементального и дифференциального копирования яв­ляется проблема выбора надежного критерия модификации файла. Обыч­но в качестве такового выступает атрибут Archive(для системDOS/Windows), время создания/модификации файлов, размер файла или контрольная сумма содержимого файла. К сожалению, все они имеют те или иные недостатки, свя­занные с особенностями обработки атрибутов и прав доступа отдельными при­кладными программами.

**Примечание**

*Некоторые из современных программных средств резервного копирования предлагают принципиально иной подход к созданию резервных копий, который иногда называют копированием на лету. Его идея состоит в том, что любые изменения файлов, указан­ных пользователем при настройке программы, сразу переносятся в резервную копию. При очевидной простоте метода, он обладает целым рядом недостатков. Основной из них заключается в том, что произведенные изменения могут быть обусловлены ошибочными дей­ствиями пользователя или работой вредоносных программ. В результате возврат к «правильной» версии файла может оказаться невозможным.*

http://www.studfiles.ru/html/2706/814/html_dhde4e9AVx.LiOQ/htmlconvd-kyidDy_html_m7eaa7d36.gif

**Н**http://www.studfiles.ru/html/2706/814/html_dhde4e9AVx.LiOQ/htmlconvd-kyidDy_html_m5d4807ee.gif**едели**

Рис. Схема дифференциального резервного копирования для недельно-­  
го цикла

Другая проблема связана с выбором периодичности создания частичных копий и с числом таких копий внутри полного цикла.

С одной стороны, чем чаще выполняется копирование, тем более «свежая» ин­формация будет сохранена в качестве резервной копии. С другой стороны, ка­ждый сеанс резервного копирования требует определенных дополнительных затрат: и времени, и резервных носителей.

Для оптимизации числа используемых резервных носителей разработаны спе­циальные алгоритмы замены носителей (так называемые *схемы****ротации но­сителей).***Наиболее часто используют следующие схемы:

* одноразовое копирование;
* простая ротация;
* «дед, отец, сын»;
* «Ханойская башня»;
* «10 наборов».

**Одноразовое копирование**- это наиболее простая схема, которая, по сути, вообще не предусматривает ротации носителей. При ее использовании резер­вируемые данные каждый раз копируются на один и тот же перезаписываемый носитель (например, наCD-RWили на дискету). Другой вариант применения такой схемы- когда очередная копия данных помещается на новый не перезаписываемый носитель (например, на СD-R). Такая схема обыч­но используется в тех случаях, когда объем резервируемых данных невелик, либо когда резервирование не носит регулярного характера (например, когда создается единственная резервная копия системы наCD-R).

**Простая ротация**подразумевает, что некий набор носителей используется циклически. Например, цикл ротации может составлять неделю, и тогда один носитель выделяется для определенного рабочего дня недели. При такой схеме полная копия обычно делается в пятницу, а в другие дни - частичные копии (инкрементальные или дифференциальные). Таким образом, для недельно­го цикла достаточно иметь пять носителей. После завершения цикла все повто­ряется сначала, и запись производится на те же самые носители. Недоста­ток данной схемы в том, что она не очень хорошо подходит для ведения архива полных копий, поскольку количество носителей в архиве быстро растет. Кроме того, достаточно частая перезапись частичных копий на одни и те же носители ведет к износу последних и, соответственно, повышает вероятность их отказа.

**Схема *«дед,*отец, сын»**имеет иерархическую структуру и предполагает ис­пользование комплекта из трех наборов носителей. Раз в неделю делается пол­ная копия дисков компьютера, ежедневно же проводится инкрементальное (или дифференциальное) копирование. Дополнительно раз в месяц произво­дится еще одно полное копирование. Набор для ежедневного инкрементально­го копирования называется «сыном», для еженедельного - «отцом», а для еже­месячного - «дедом». Состав носителей в ежедневном и еженедельном наборах является постоянным. При этом в ежедневном наборе каждый носитель соот­ветствует определенному дню недели, а в еженедельном наборе – каждой неделе месяца. Носители из «ежемесячного» набора обычно заново не исполь­зуются и откладываются в архив. Недостаток данной схемы состоит в том, что в архиве находятся только данные, имевшиеся на конец месяца. Как и при про­стой ротации, ежедневные копии подвергаются значительному износу, в то время как нагрузка на еженедельные копии сравнительно невелика.

**Схема «Ханойская башня»**редко используется пользователями «домашних» компьютеров. Она построена на применении нескольких наборов носителей. Их количество не регламентируется, но обычно ограничивается пятью-шестью. Каждый набор предназначен для недельного цикла копирования, как в схеме простой ротации. Каждый набор содержит один носитель с полной недельной копией и носители с ежедневными инкрементальными (дифференциальными) копиями. В таблице приведена схема ротации для пяти наборов носителей.

Схема ротации «Ханойская башня» для 5 наборов носителей



Каждый следующий по порядку набор используется в два раза реже, чем пре­дыдущий. Таким образом, набор N1 перезаписывается каждые две недели, на­бор N2 - каждые четыре недели, и т. д.

**Схема «10 наборов»**также используется нечасто. Как следует из названия, схема рассчитана на использование 10 наборов носителей. Период из 40 недель делится на десять циклов. В пределах цикла за каждым набором закреплен один день недели. По прошествии четырехнедельного цикла осуществляется переход к следующему набору. Например, если в первом цикле понедельнику соответствовал набор 1, а за вторник - набор 2, то во втором цикле понедель­нику будет соответствовать набор 2, а вторнику - набор 3. Такая схема позво­ляет равномерно распределить нагрузку и, как следствие, выровнять износ но­сителей.

**Программно-технические средства резервного копирования**

Существующие в настоящее время программы резервного копирования избав­ляют пользователей и системных администраторов от необходимости «вруч­ную» отслеживать периодичность создания **и**обновления резервных копий, за­мены носителей и т. п. Правда, перечень предоставляемых такими программа­ми сервисных возможностей существенно зависит от категории программы. Все программы резервного копирования можно условно разделить на три кате­гории:

• Системы начального уровня, включаемые в состав операционных сис­тем. К ним можно также отнести большинство бесплатных и условно- бесплатных программ резервного копирования. Эти программы предна­значены для индивидуальных пользователей и небольших Организаций.

* Системы среднего уровня; при относительно невысокой цене они обла­дают широкими возможностями по резервному копированию и архива­ции данных. Подобных систем довольно много (в частности, ARCserveITкомпанииComputerAssociates,BackupExecотSeagateSoftwareиNetWorkerкомпанииLegatoSystems).
* Системы верхнего уровня предназначены для резервного копирования и архивирования в сложных гетерогенных средах. Они поддерживают разнообразные аппаратные платформы, операционные системы, базы данных и приложения корпоративного уровня, имеют средства интегра­ции с системами управления сетью и обеспечивают возможность ре­зервного копирования/архивирования с использованием разнообразных типов накопителей. К подобным системам можно отнести ADSMком­пании ЮМ иOpenViewOmniBackIIотHewlettPackard. Однако для многих организаций (не говоря уже об индивидуальных пользователях) они весьма дороги.

Одной из важных характеристик программ резервного копирования является перечень поддерживаемых типов сменных носителей.

Вместе с тем, при создании резервной копии в «ручном» режиме, вы вольны использовать любое из существующих на сегодняшний день устройств хране­ния данных. Их перечень с краткой характеристикой приведен в табл.

Устройства хранения данных, применяемые при резервном копи­ровании

|  |  |  |
| --- | --- | --- |
| **Тип устройства** | **Достоинства** | **Недостатки** |
| Жесткий диск (HDD) | Б. емкость, быстродействие (), высокая надежность, долговечность, многократная перезапись, низкая стоимость, возможность загрузки резервной копии | Ненадежность при транспортировке, воздействие ЭМ излучений, (подключение ..) |
| CD-R,CD-RW | Приемлимое быстродействие и скорость , н. стоимость, надежность, долговечность | Емкость, Не все виды ПК оснащены |
| DVD | Большая емкость, тоже что CD… | Специализация, Не все виды ПК оснащены |
| Карты памяти SD,MS, (CF),MMC,… | Емкость, скорость, надежность, Приемлимое быстродействие и скорость, возможность использования для переноса м-ду разнотипными устр |  |
| Модули флеш памяти | То же |  |
| Внешний жесткий диск | USB |  |
| *MobileRack,*  *Стример, флоппи, ZIP,ZIV, магнитооптические* |  |  |

Краткие итоги сравнительной оценки параметров представленных в таблице носителей.

Та или иная схема ротации может быть реализована только для уст­ройств со сменными носителями, к числу которых относятся оптические (CDиDVD) (и магнитооптические диски). При этом для «среднестатистического» пользователя один носитель ем­костью в несколько гигабайт явно «великоват» для хранения одной копии данhttp://www.studfiles.ru/html/2706/814/html_dhde4e9AVx.LiOQ/htmlconvd-kyidDy_html_3effe108.gifных. Единственное исключение - когда речь идет о создании образа цело­го раздела жесткого диска.

Таким образом, по совокупности характеристик оптимальным вариантом на сегодняшний день можно считать резервное копирование на базе перезапи­сываемых оптических дисков (CDилиDVD).

Относительно использования жесткого диска в качестве резервного носителя необходимо сделать несколько дополнительных замечаний.

Первое: если имеется необходимость хранить жесткий диск с резервной копией данных отдельно от компьютера, на котором они создавались, то целесообраз­но использовать (так называемый *переносной диск*(MobileRack) жесткий диск сUSBинтерфейсом. .

Второе: если ваш компьютер работает под управлением операционной системы WindowsXPProfessional, и на нем установлены как минимум два жестких дис­ка, вы можете использовать отказоустойчивые технологииRAID-1 иRAID-5.

Третье: при наличии единственного жесткого, диска достаточно большой емко­сти целесообразно разбить его на несколько логических разделов, один из ко­торых (по крайней мере) может быть использован в качестве резервного диска; такой логический резервный диск будет защищен от многих напастей, грозя­щих «рабочим» разделам (хотя, разумеется, далеко не от всех);

***Технология RAID***

*В достаточно крупных организациях для резервного копирования критически важных данных применяется технология RAID(RedundantArrayofIndependedDisks- избыточный массив независимых дисков), основанная на системе спе­циальным образом сконфигурированных жестких дисков. Исходной целью создания технологииRAIDявлялось повышение производи­тельности дисковой памяти за счет использования нескольких взаимосвязан­ных жестких дисков вместо одного.*

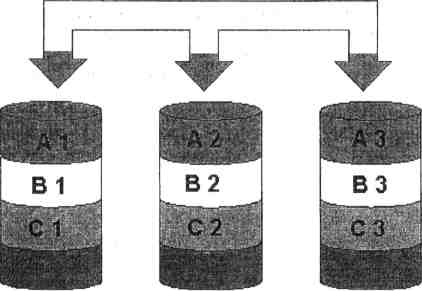
*Всего на сегодняшний день промышленными стандартами предусмотре­но восемь уровней (модификаций) RAID:*

* *RAID-0- объединение пространства нескольких физических дисков в один виртуальный том, для которого применяется метод чередования (striping, отstrip- «полоса»): информация делится на блоки, поочеред­но записывающиеся на все накопители тома (рис. 4.3).RAID-0 обеспе­чивает высокую скорость обмена данных, но надежность виртуально­го тома несколько ниже, чем у любого другого уровня и ниже надежно­сти каждого из входящих в том дисков, так как при выходе из строя хотя бы одного из них вся информация теряется.*

*RAID-1 - дублирование, или «зеркалирование» (mirroring- зеркальное отражение) дисков. В этом случае информация одновременно записыва­ется на два (как правило) диска. При выходе из строя одного из них данные считываются с «зеркала». К этому уровню относят также при­менение дуплексных томов (DuplexVolume), когда физические диски, используемые в качестве зеркал, обязательно должны быть подключены к разным контроллерам. Реализация восстановления после сбоев при использованииRAID-1 достаточно проста, однако имеет место высокая (100%) избыточность.*

*RAID-2 - предполагает создание на основе нескольких физических дис­ков одного массива (тома), данные в который записываются с использованием контрольного кода (кода Хемминга). Для хранения контрольных кодов отводится специально выделяемый диск.RAID-3 - массив с чередованием и использованием кода четности для обнаружения ошибок. Информация о четности, как и в случаеRAID-2, хранится на отдельном диске, но имеет меньшую избыточность.RAID-4 - подобен уровню 3, но данные разбиваются на блоки, записы­вающиеся на разные диски, причем возможно параллельное обращение к нескольким блокам, что существенно повышает производительность.RAID-5 - аналогичен уровню 4, но информация о четности хранится не на выделенном диске, а циклически распределяется между всеми дис­ками тома.*

*RAID-6 - в отличие от уровня 5, использует две независимые схемы четности, что увеличивает как избыточность, так и надежность хранения информации.*



*RAID-7 - отказоустойчивый массив, оптимизированный для повышения производительности. Данный уровеньRAIDподдерживается лишь спе­циализированными ОС.*

*Диск 2*

*Том RAID*

*Рис. Схема использования RAID-0*

*Технология RAIDна сегодняшний день реализуется как на аппаратном уровне, так и программно.*

*Аппаратная реализация является более эффективной и основа­на на подключении жестких дисков через специальные RAID-контроллеры. Такой контроллер выполняет функции связи с сервером (рабочей станцией), генерации избыточной информации при записи и проверки при чтении, рас­пределения информации по дискам в соответствии с алгоритмом функциони­рования.*

*Принцип работы программно управляемого тома RAID-1 состоит*

*в следующем.*

*На основе двух разделов, расположенных на двух разных физических дисках, создается так называемый зеркальный том (MirrorVolume). Ему присваивается собственная буква диска (исходные разделы дисков лишаются таковой вооб­ще), и при выполнении каких-либо операций над данными этого тома все из­менения синхронно отражаются в обоих исходных разделах. При выходе из строя (отказе или сбое) одного из двух дисков система автоматически пере­ключается на работу с оставшимся в живых «последним героем». При возник­новении такой ситуации пользователь может разделить зеркала, и затем объе­динить исправный раздел с другим разделом в новый зеркальный том. В зеркальный том можно включить практически любой раздел, в том числе системный и загрузочный.*

**Восстановление данных по резервным копиям**

Можно еще и еще повторять, что использование резервного копирования дан­ных - это наиболее простой и надежный способ обеспечения их сохранности. Тем не менее, многие пользователи предпочитают сэкономить несколько ми­нут на создании резервной копии, чтобы потом потратить несколько часов (или даже дней) и уйму нервных клеток на восстановление утраченной информации. Тем более странно мириться с этим сегодня, когда существует масса инстру­ментальных средств, требующих от пользователя всего лишь указать «когда, чего и сколько» резервировать.

При выборе конкретного инструмента резервного копирования целесообраз­но учитывать следующие факторы:

* перечень реализованных методов резервного копирования;
* поддерживаемые типы носителей данных;
* удобство использования (качество пользовательского интерфейса).

Технология работы практически всех программ резервного копирования одно­типна: пользователь создает так называемое задание, в котором указывается состав копируемых данных, метод резервирования (полное, добавочное или разностное), периодичность создания копии, ее расположение и (возможно) некоторые другие параметры. Для восстановления данных (конкретного файла или целого диска) требуется указать, какую копию следует использовать, и за­дать режим обновления (с заменой оригинала или без таковой). Такая технология применима как при восстановлении «пользовательских» дан­ных, так и системной информации. Тем не менее, восстановление системной информации имеет определенные особенности, которые будут рассмотрены в главе «Восстановление данных».

Ниже в качестве примера коротко рассмотрены два стандартных (а потому наиболее доступных) инструмента резервного копирования и восстановления, входящие в состав WindowsXPProfessional:программа*Архивация данных*и программа *Восстановление системы.*Первая из них является более «универ­сальной», и может быть использована для любых наборов данных, вторая име­ет более специфическое предназначение - восстановление системных парамет­ров.

**Программа Архивация данных (WindowsXPProfessional)**

Версия программы *Архивация данных,*входящая в составWindowsXPProfessional, поддерживает различные виды носителей, что позволяет выпол­нять резервное копирование на любое запоминающее устройство, поддержи­ваемое операционной системой. К числу таких устройств относятся любые гибкие или жесткие диски, магнитооптические накопители и другие устройства (а не только стримеры, как в версии этой программы дляWindows98).

Примечание

*Чтобы использовать программу резервного копирования, необходимо за­пустить службу Съемные ЗУ. Как и любая другая служба WindowsXPProfessionalона может быть запущена с консоли администрирования системы.*

В WindowsXPдля создания резервной копии данных используются так называемые*моментальные снимки тома*(volumesnapshots). Суть техно­логии состоит в следующем. На момент инициации процедуры резервно­го копирования создается снимок тома. После этого данные резервируются, но не с исходного тома, а с его снимка. Это позволяет сохранить возможность доступа к файлам во время процесса резервного копирования.

Программа *Архивация данных*(рис. 4.4) обладает следующими основными воз­можностями:

* резервное копирование данных в разделах с файловыми системами NTFS,FATиFAT32, причем как для локальных, так и для сетевых дис­ков;
* создание резервных копий как для отдельных файлов и папок, так и для всех логических дисков компьютера;
* дополнительная проверка целостности созданной резервной копии и ре­зультатов восстановления;
* поддержка трех «классических» видов резервного копирования (полно­го, инкрементального и дифференциального), а также специального ви­да - ежедневного;
* создание командного файла (bat-файла), позволяющего автоматизиро­вать процесс резервного копирования;
* проведение резервного копирования по расписанию;

ведение журнала процедур резервного копирования и восстановления

Особо следует отметить наличие мощной поддержки резервного копирования и восстановления системных данных. Для восстановления работоспособности операционной системы WindowsXPиспользуются два набора данных: систем­ные файлы, сохраненные на ленте или другом носителе, а также информация о конфигурации жесткого диска, сохраненная на специальной дискете

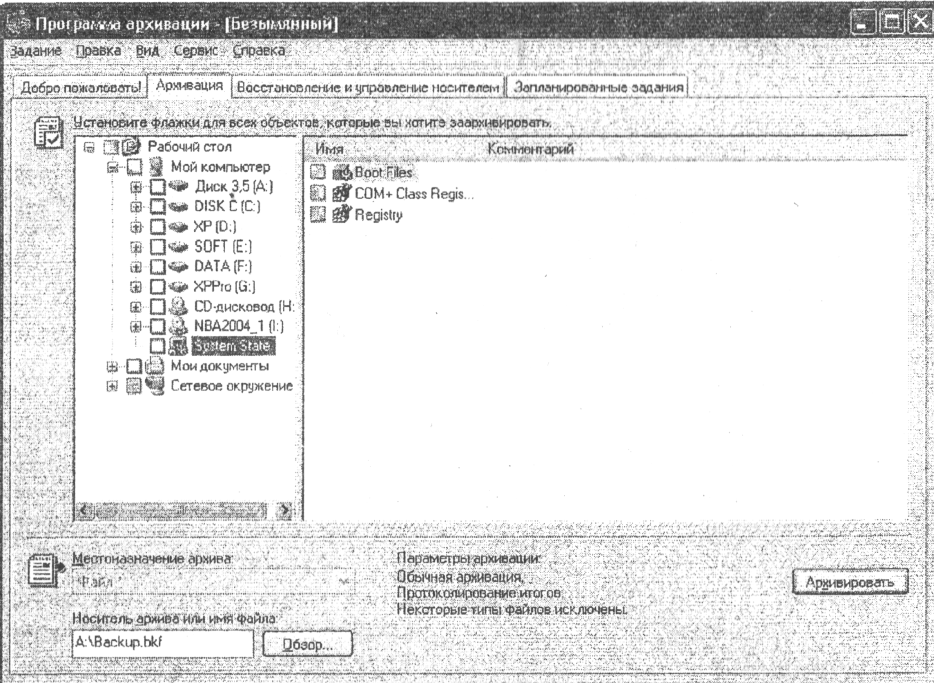


Рис. Основное окно программы *Архивация данных*

***Программа Восстановление системы***

*Работа этого инструмента основана на создании так называемых то­чек****восстановления.***

*Точка восстановления представляет собой «снимок» текущих значений основ­ных параметров системы, в том числе реестра, параметров Рабочего стола и некоторых других. Соответственно, процедура восстановления состоит в замене используемых параметров системы на те, которые были зафиксирова­ны в точке восстановления.*

*По умолчанию программа Восстановление системы сама выбирает момент для создания точки восстановления. В частности, новая точка создается перед ус­тановкой на компьютер нового программного обеспечения или перед измене­нием конфигурации устройств (на уровне драйверов). Тем не менее, пользова­тель в любой момент может дать указание программе создать новую точку вос­становления.*

*Программа Восстановление системы не позволяет отменить изменения, связанные с созданием/удалением разделов и логических дисков.*

*Программа реализована в виде своеобразного мастера (рис. 4.5), который по­зволяет создать новую точку восстановления, выбрать одну из имеющихся, чтобы восстановить систему, а также открыть панель настроек программы. Для восстановления требуемого состояния системы достаточно выбрать соот­ветствующую точку восстановления, и затем следовать указаниям мастера про­граммы.*

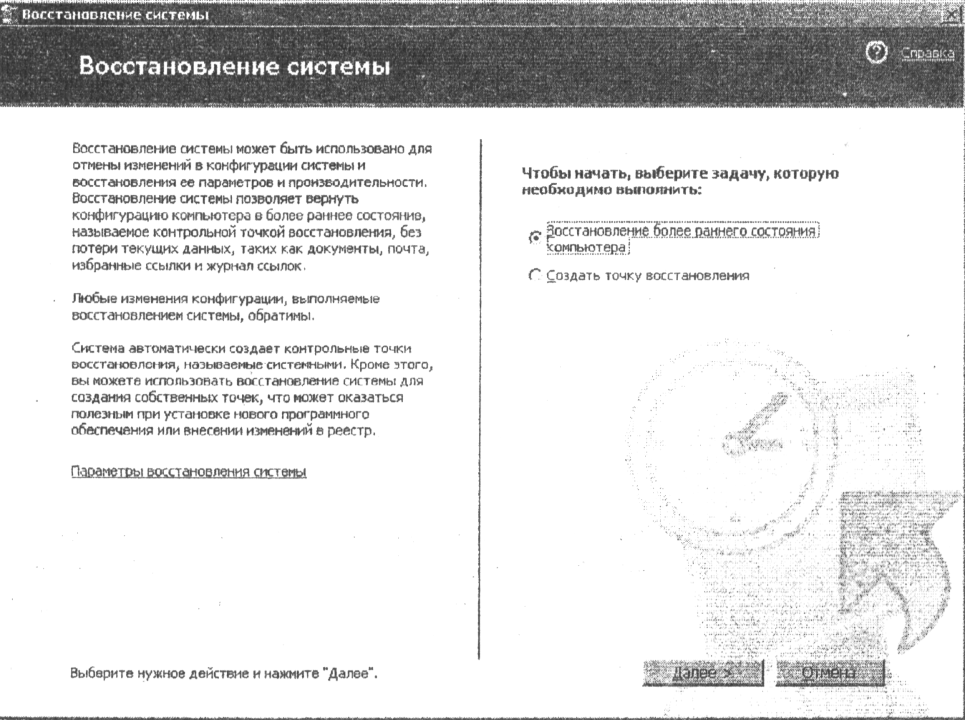


Рис. Стартовое окно программы *Восстановление системы*

**Настройка системных параметров**

Как вы, вероятно, помните, одной из наиболее серьезных угроз безопасности данных является так называемый «человеческий фактор». Ошибка, допущен­ная по невнимательности или по какой-то другой причине, может зачастую на­нести больше вреда, чем самый страшный вирус. Поэтому полезно приучить себя к соблюдению некоторых правил, призванных снизить риск потери дан­ных.

Первое, о чем следует позаботиться - это возможность загрузки системы с резервного носителя в случае ее «краха». Для установки соответствующих параметров потребуется познакомиться с BIOS.

Второй важный момент - это правильная организация работы с жесткими дис­ками. Какие бы альтернативные виды накопителей ни привлекали ваше внима­ние, ключевую роль в хранении данных и обеспечении работы системы в целом по-прежнему играют «винчестеры». Поэтому для уверенной и кор-ректной работы с данными весьма полезно представлять себе, как, собственно, выглядит файловая система «изнутри».

И, наконец, третья составляющая 4- это установка рациональных значений па­раметров, относящихся к пользовательскому интерфейсу файловой системы. Привыкнув решать многие задачи «буквально двумя щелчками мыши», мы не всегда даже обращаем внимание на ответную реакцию системы. А ведь ино­гда, в ответ на бурное наше негодование по поводу удаленного файла или «за­висания» системы, она вполне могла бы заметить: «Мы ведь вас предупреждали...».

Так о чем же пойдет речь в этом подразделе? Он содержит набор практических рекомендаций, призванных обеспечить снижение вероятности потери или по­вреждения информации из-за некорректных или нерациональных значений системных параметров.

***Установка параметров BIOS***

*BIOS(BasicInput/OutputSystem- базовая система ввода-вывода) - это специ­альная программа, которая хранится в энергонезависимом ПЗУ (постоянном запоминающем устройстве) материнской платы и обеспечивает инициализа­цию загрузки системы, а также выполнение некоторых других функций, о которых будет сказано ниже.*

*Используемые в настоящее время BIOSимеют несколько десятков настраивае­мых параметров, из которых нас будут интересовать только имеющие отноше­ние к восстановлению работоспособности системы.*

***Примечание***

*Для настройки параметров BIOSиспользуется специальная программа -BIOSSetup. Она хранится в том же ПЗУ, что и самаBIOS. Способ акти­визацииBIOSSetupзависит от особенностей материнской платы, но обычно для этого достаточно нажать на клавиатуре клавишу <Del> сразу после завершения (или даже во время выполнения) процедуры само­тестирования материнской платы.*

***Параметры загрузки системы***

*Первый интересующий нас параметр определяет набор устройств, с которых разрешена загрузка операционной системы, и последовательность поиска таких устройств в составе компьютера. Параметр входит в раздел, который в программе BIOSSetupот компанииAwardназываетсяBIOSFeaturesSetup(установка параметровBIOS), а в варианте компанииAMI-AdvancedCMOSSetup(дополнительные параметрыCMOS).*

*Наименование данного параметра и перечень его возможных значений опять-таки зависят от версии используемой программы BIOSSetup. В некоторых вер­сияхBIOSSetupдля указания последовательности просмотра системных уст­ройств используется набор взаимосвязанных параметров. Выбор наиболее под­ходящего варианта зависит от реальной конфигурации компьютера, а также от типа используемых системных резервных носителей*

*Параметры антивирусной защиты и контроля доступа*

*Практически все современные BIOSсодержат в своем составе средства диагно­стики и/или защиты системного жесткого диска от вирусов. Защита заключается в том, чтоBIOSконтролирует поведение программ, пы­тающихся что-либо изменить в системной области диска. Соответственно, за­щита, реализуемаяBIOS, направлена в первую очередь против загрузочных ви­русов.*

*С помощью BIOSSetupвы можете разрешить или запретить такую защиту. Наименования соответствующих параметров также зависят от версииBIOSSetup, но практически везде они входят в разделBIOSFeaturesSetup(вBIOSот компанииAward) илиAdvancedCMOSSetup(в варианте компанииAMI).*

*С точки зрения борьбы с вирусами имеет достаточно важное значение еще од­на особенность современных BIOS. Речь идет о том, что производителиBIOSстремятся повысить их адаптивность к быстро изменяющимся «типовым» кон­фигурациям компьютеров. С этой цельюBIOSчасто записывается не в ПЗУ, содержимое которого можно изменить только с помощью специального уст­ройства - программатора, а в перезаписываемые микросхемы (flash), содержи­мое которых можно изменить программно. Разумеется, создатели виру­сов не преминули использовать возможность напакостить пользователям, ис­портив содержимоеFlashBIOS. Так вот, при наличии в настройкахBIOSпара­метраFlashBIOSProtection(защитаFlashBIOS) его обязательно следует уста­новить в положениеEnabled(разрешено). В этом случае микросхемаFlashBIOSбудет закрыта для записи.*

***Восстановление данных***

Хотя резервное копирование данных и правильная настройка системных пара­метров помогают предотвратить множество проблем, в некоторых ситуациях эти меры оказываются бессильны. Например, когда сделанные в документе из­менения оказались утеряны из-за сбоя системы еще до их переноса в резервную копию. Или когда системный реестр оказался поврежден из-за от­ключения электропитания во время загрузки системы.

В подобных случаях для восстановления данных необходимо использовать специальные инструментальные средства.

**Восстановление данных пользователя**

Иногда для восстановления собственных файлов с данными пользователю при­ходится предварительно восстанавливать работоспособность всей системы. Разработчики программных средств восстановления прекрасно знают об этом, и потому многие инструментальные средства и приемы, рассмотренные в этой главе, пригодны также для восстановления системной информации. Одна­ко значительно чаще удаленный случайно файл можно восстановить с минимальными затратами времени и сил, не прибегая к сложным процеду­рам. Для таких случаев вполне можно подобрать пару программных инстру­ментов, отвечающих вашим вкусам и потребностям, и не требующих работы с данными на уровне двоичных или шестнадцатеричных кодов. Тем не менее, начнем мы все-таки с пояснения некоторых технических деталей.

Введение в технологию реанимации

В «воскрешении» удаленных или испорченных файлов нет ниче­го мистического.

Еще с незапамятных времен безраздельного господства на компьютерах IBMPCоперационной системыMS-DOSи файловой системыFATоперация «уда­ление файла» сводится к выполнению очень простого приема. Заключается он в том, что в дескрипторе файла, хранящемся в каталоге-держателе файла, все­го лишь изменяется первая буква имени файла. Вместо нее записывается шест-надцатеричный код Е5, дающий при отображении на экране символ «х»

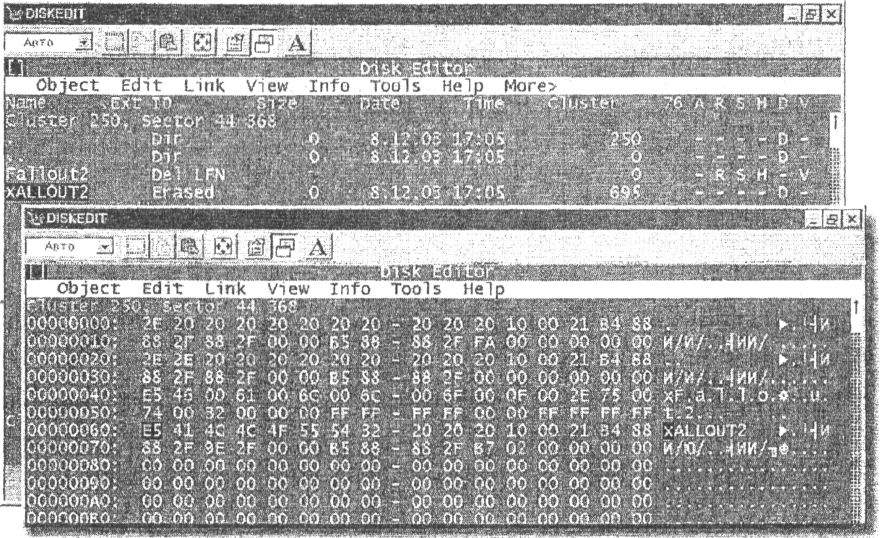


Рис.. Признак удаления файла - код Е5 в первом байте имени

Такой файл получает признак «удаленный» (Erased), а распределенные ему кластеры считаются свободными. Никаких других изменений в области данных диска не происходит. Соответственно, для восстановления файла достаточ­но выполнить обратную замену кода Е5 на исходную букву имени

http://www.studfiles.ru/html/2706/814/html_dhde4e9AVx.LiOQ/htmlconvd-kyidDy_html_m6663b0f5.gifСказанное относится и к удалению папок: удаленная папка остается на прежнем месте, включая все содержимое. Заменяется лишь первый байт имени папки (кодом Е5) в соответствующей записи родительского каталога. Процедура восстановления заключается в выполнении той же операции обрат­ной замены первого байта имени.

**Примечание**

*По указанной выше причине «обычное» удаление файлов с конфиденциальными данными не помешает заинтересованным ли­цам без труда прочесть эти данные. Для действительного уничтожения данных существуют специальные программы-«затиратели», которые прописывают в кластеры удаленного файла новый код, причем много­кратно. Обычно такие программы называют шредерами (от Schrader), по аналогии со специальными устройствами для физическо­го уничтожения бумажных документов. Восстановить данные, над ко­торыми поработала программа-шредер, практически невозможно. Разве что с помощью инструментов, имеющихся в распоряжении спецслужб.*

Правда, такая «реанимация» возможна только до тех пор, пока освободившиеся кластеры не будут отданы какому-либо новому файлу. Поэтому, если вы слу­чайно удалили файл (минуя *Корзину)*или потеряли его в результате каких-то других действий,**выполните следующие профилактические меры**:

* Убедитесь, что файл действительно удален; помните, что зачастую име­ет место «ложная тревога», когда файл, например, оказывается про­сто перемещен или переименован;
* Постарайтесь «по горячим следам» уточнить, при каких обстоятельст­вах был потерян (удален) файл. Если причина не очень понятна и вызы­вает определенные опасения, создайте внеочередную резервную копию наиболее важных данных, но (обязательно!) на другом запоминающем устройстве.
* Не записывайте на логический диск с потерянными данными новых файлов и не создавайте на нем новых папок.
* Как дополнение к предыдущему пункту - не устанавливайте на этот диск новых программ, в том числе утилит, с помощью которых вы со­бираетесь спасать свои данные; многие из таких утилит способны рабо­тать непосредственно с дискеты или с компакт-диска.
* Если на компьютере имеются сервисные программы, которые запуска­ются по расписанию (например, программа дефрагментации диска или программа резервного копирования), предотвратите их возможный за­пуск и остановите работу программ, выполняющих мониторинг системы (в частности, менеджер задач); особенно опасна в такой ситуации про­цедура дефрагментации, которая существенно снижает вероятность ус­пешного восстановления.

По возможности, не перезагружайте компьютер. Правда, если диск с потерянными данными не является системным, это требование не обязательно для выполнения. Более того, для использования некоторых утилит восстановления потребуется перезагрузить систему для работы в однозадачном режиме (под управлением DOSили другой однозадач­ной ОС). Поэтому после того, как данные будут успешно восстановле­ны, оцените еще раз, насколько удачна используемая вами конфигура­ция логических дисков.

Возможно, «пропажа» нужных данных будет обнаружена не сразу, а через не­которое время (скажем, через пару дней), когда вы уже успеете записать на диск новые файлы или создать новые папки. Но даже и в этом случае еще далеко не все потеряно. Дело в том, что система пытается распределять в пер­вую очередь дисковое пространство, которое ранее не использовалось, и лишь при необходимости выделяет под новые данные кластеры, «бывшие в употреблении». Это позволяет, используя информацию из таблицы распреде­ления файлов (FAT), выявить уцелевшие фрагменты цепочки кластеров уда­ленного файла и затем собрать их в одно целое. Восстановленный файл не все­гда будет иметь первозданный вид, но иногда и такой результат может быть расценен как успех.

«Очень плохая» ситуация возникает в результате ***полного форматирования диска.***Полное форматирование приводит не только к обновлению системных областей, но и к прописыванию области данных служебным кодом. Объясняет­ся это тем, что в ходе полного форматирования производится проверка физиче­ского состояния секторов диска, основанная на записи/считывании в них слу­жебного кода.

Однако удаление данных - это лишь один из возможных видов нарушения их целостности. Чаще данные оказываются повреждены частично. Например, для многих графических форматов достаточно критичным является состояние пер­вых нескольких байтов, в которых содержится описание формата

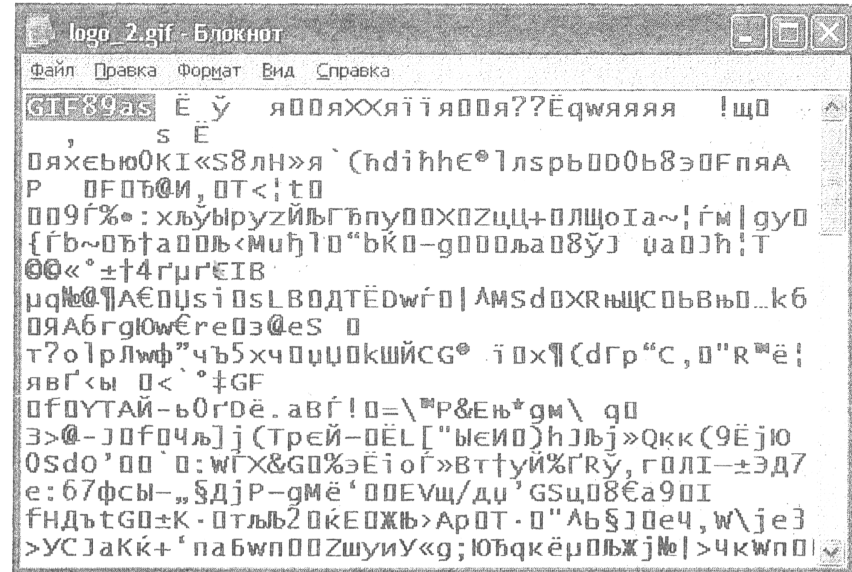


Рис. Первые байты графического файла в формате GIFсодержат описание формата

И если даже собственно изображение не повреждено, искажение этих бай­тов может сделать его недоступным для просмотра.

Процедура выявления подобных ошибок называется ***контролем целостности***данных. Ее выполнение может быть возложено либо на отдельные модули, входящие в состав различных приложений, либо па специальные утилиты.

Программы контроля целостности данных

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

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

Примечание

*Иногда аббревиатуру CRC интерпретируют как «контрольная сумма», что неверно, поскольку вычисление контрольной суммы для некоторо­го блока данных*-*это альтернативный метод проверки, более простой и менее надежный. Вычисление лее CRC основано на использовании специ­ального "магического" полинома, коэффициенты которого определяются в соответствии с используемым алгоритмом CRC*

Обычно длина значения CRCсоставляет 16 или 32 двоичных разряда. 32-разрядную контрольную свертку для определенности обозначаютCRC-32, а само значение представляют в шестнадцатеричном коде.

Использование CRC-32 обеспечивает очень высокую достоверность контроля. Достаточно изменить единственный бит в контролируемом файле, и значение контрольной свертки станет совершенно другим. Например, взгляните на зна­ченияCRC-32 для двух текстовых файлов, различающихся одним битом (рис. 4.13).

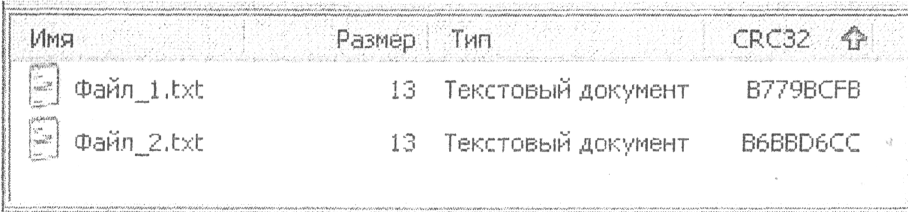


Рис. Значения CRC-32. для двух файлов

В отличие от контрольных сумм, метод CRCсможет распознать всякие фокусы с перестановкой двух байт либо с добавлением 1 к одному из них и вычитани­ем 1 из другого.

Механизм CRCчрезвычайно полезен для проверки файлов, загружаемых из сетевых информационных служб. Например, если утилита, перенесенная с одного компьютера на другой через сетьIntranet, вдруг без видимой причины перестает работать, то первым делом следует сравнить значение парамет­ровCRCдля оригинала и копии утилиты. Если вычисленное значение пара­метраCRCне совпадает со значением для исходного варианта файла, значит, при загрузке его произошла необнаруженная ошибка передачи данных

Программ, обеспечивающих контроль целостности данных на основе вычисле­ния CRC, известно достаточно много. Большинство из них бесплатны или ус­ловно-бесплатны. В разных программах могут использоваться различные алго­ритмы вычисленияCRC, однако принцип работы таких программ один: снача­ла программа вычисляет контрольную свертку для каждого из указанных фай­лов (или папок), а затем при повторном запуске (по «велению» пользователя или по расписанию) выполняет повторный расчетCRCи сравнивает получен­ное значение с тем, которое хранится в базе данных программы. Необходимо отметить, что утилиты контроля целостности данных на основеCRCчасто входят в состав более сложных и мощных программ. В частности, анализCRCконтролируемых файлов выполняют антивирусные пакеты (с целью выявления факта несанкционированного изменения этих файлов). В программах-архиваторахCRCиспользуется для контроля целостности архи­ва

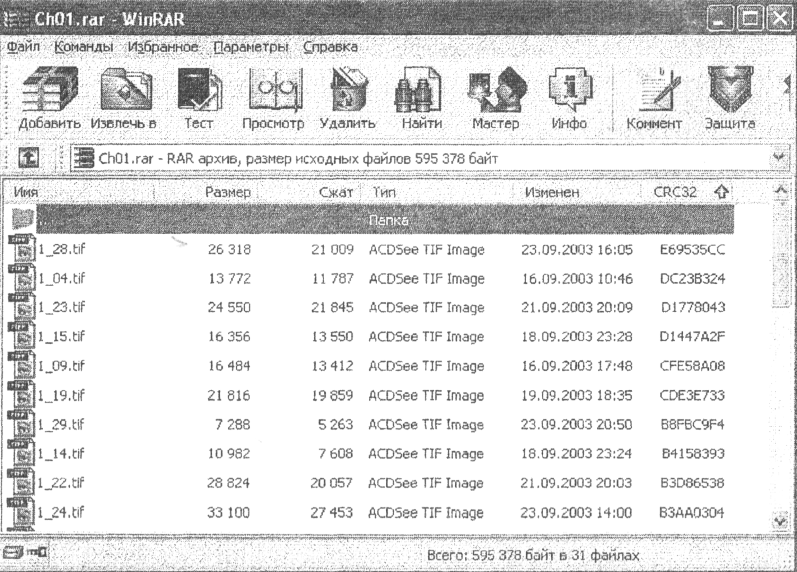


Рис. Архиватор WinRARвычисляет контрольную свертку для архивируе­мых файлов

Программы, имеющие в своем составе модули вычисления контрольной сверт­ки, обычно умеют и восстанавливать поврежденные данные. Однако такие возможности ограничены, как правило, лишь конкретными форматами файлов. Например, упомянутый выше архиватор WinRARумеет восстанавливать ар­хивные файлы, а текстовый процессорMSWord- лишь свои, «вордовские», документы. Значительно более мощными возможностями обладают специаль­ные программы восстановления данных.