**Восстановление информации на жестком диске**

Настоящий обзор не является техническим руководством по изучению строения жестких дисков или описанием их логических структур. Это общий обзор методик и способов восстановления информации, ставшей недоступной в результате программного сбоя операционной системы, разрушительного действия вируса или неосторожных действий пользователя.

Несколько общих слов о строении и терминологии жестких дисков.

Жесткий Диск (винчестер) представляет собой блок из нескольких дисков/блинов (Disks) по поверхностям (Sides) которых перемещаются (плавают в воздушном потоке) головки (Heads). Позиционируются головки по концентрическим дорожкам/трекам/цилиндрам (Cilinders), каждый из которых разделен на сектора (Sectors). Сектор является минимальным адресуемым блоком данных для диска и его размер равен 512 байтам. Логическое строение жесткого диска отличается от его настоящей (физической) геометрии и это необходимо учитывать при восстановлении информации. Как правило, современные диски (в режиме адресации LBA) представляют собой несколько сот цилиндров имеющих 63-254 поверхностей по 63 сектора данных на каждой.

В самом начале диска (в секторе 0/0/1) находитсяPT (Partition Table) - таблица разделов и MBR (Master Boot Record) - главная загрузочная запись.

На следующем треке в первом(ых) секторе(ах) (начиная с 0/1/1) расположена BA (Boot Area) - загрузочная область операционной системы и BR (Boot Record) - загрузочная запись OC.

Далее на этом же треке расположена 1-я копия FAT(File Allocation Table) - таблица размещения файлов. Сразу за ней - 2-я копия FAT. Размер копии FAT (в секторах) определяется размером раздела диска.

После 2-й копии FAT расположены сектора ROOT (Root directory) - корневого каталога, за которой начинается DA (Data Area) - область данных.

PT - состоит из 4-х строк описывающих 4-е возможных раздела диска. Описание каждого раздела диска содержит информацию о типе файловой системы, признаке того, что раздел является загрузочным, о первых и последних головках, дорожках, секторах раздела, количестве секторов смещения начала раздела от начала диска и об общем количестве секторов в разделе.

MBR - находится в том же секторе что и PT. Данные в MBR представляют собой код процессора необходимый для дальнейшей загрузки операционной системы. В последних двух байтах сектора MBR находится сигнатура 55AAh, которую можно использовать как маску при поиске PT и MBR.

BR - содержит массу данных и служит для описания параметров файловой системы. В отличие от диска, минимальным адресуемым блоком данных для операционной системы служит кластер, объединяющий определенное количество секторов. В BR нам интересны такие данные как размер кластера, размер и количество копий FAT. BR для раздела FAT16 размещается в одном секторе, в случае FAT32 Boot Record состоит из нескольких секторов.

FAT - Состоит из 12, 16 или 32 битных элементов, описывающих номера кластеров или их признаки (BAD). Количество элементов соответствует количеству кластеров раздела диска. Из этих элементов образуются цепочки номеров кластеров, описывающих расположение файлов на диске.

ROOT - Корневой каталог диска. Содержит записи описывающие файлы (дескрипторы файлов) в корневом каталоге. Такая запись описывает имя, тип, дату создания, размер, атрибуты файла, и т.п., а так же содержит указатель на первый кластер файла.

Каталоги представляют собой сектора идентичные по структуре корневому каталогу. Каталог, кроме описаний файлов, в самом начале содержит две записи, первая из которых содержит указатель на первый кластер самого каталога, вторая на первый кластер родительского каталога.

**Восстановление информации:**

Для восстановления потерянных (поврежденных) данных постарайтесь вспомнить или получить информацию о:

a. Вероятном разбиении диска на разделы и количестве логических дисков.

b. Размерах и истории создания логических дисков. История создания подразумевает под собой возможные искусственные изменения размеров разделов диска. Эта информация может иметь значение для точного определения места расположения ROOT.

c. Особенностях файловой системы FAT16 или FAT32. Остальные типы файловых систем в этом документе не рассматриваются.

d. Типе и версии Операционной Системы (DOS, Win95/98) использовавшейся на диске.

e. Уникальные имена директорий и файлов, находившихся в корневом каталоге диска С, имя каталога с данными, подлежащими приоритетному восстановлению и уникальные имена файлов и поддиректорий, находившихся в этой директории.

Для восстановления данных можно воспользоваться следующими утилитами:

1. DiskEdit из комплекта Norton Utilities версии 3.0х (или аналогичный ему).

2. Tiramisu или Hard Drive Mechanic.

Утилита TIRAMISU существует в различных модификациях, соответствующих разным типам файловых систем (FAT16/FAT32/NTFS/Novell/ZIP). Данная программа позволяет УвытащитьФ Ваши данные с УбольногоФ диска, необходимо только чтобы диск определялся BIOS-ом и был физически исправен. Обращаю внимание еще раз, что эта программа не лечит диск, она позволяет скопировать ваши данные на другой носитель.

3. UnFormat (из того же комплекта Norton Utilities).

4. NDD - Norton DiskDoctor (опять из того же комплекта Norton Utilities).

Возможно, применение и других утилит, но, как правило, они ограничиваются частными случаями или не учитывают всевозможных особенностей логического строения дисков.

1. ДИАГНОСТИКА ПОВРЕЖДЕНИЙ.

1.1. Запустите DiskEditor и, переведя его в режим просмотра поврежденного диска на физическом уровне, последовательно проверьте целостность РТ, MDR, FAT-ов, ROOT и DA. На этом этапе постарайтесь выяснить (если это достоверно неизвестно) тип файловой системы первого раздела диска (FAT16 или FAT32).

В стандартных случаях диски объемом менее 528 Mb, или разбитые на разделы при помощи системных утилит ДОС 7.10 и более ранних - имеют FAT16.

Операционные системы Windows 95 OSR2 и Windows 98 базирующиеся на ДОС 7.10а на дисках и разделах объемом больше 528 Mb, как правило, используются с файловой системой FAT32.

1.2. В случае целостности каких-либо элементов дисковой структуры сохраните их в виде файлов на резервном диске.

Например: MBR.HEX, BR1.HEX, FAT01.HEX, FAT02.HEX, ROOT0.HEX.

1.3 Дальнейшее восстановление диска зависит от степени и характера повреждений.

Если у Вас осталась неповрежденной (или хотя бы частично) какая-либо копия FAT на первом разделе диска - восстановление информации возможно почти в полном объеме.

2. Временное РЕЗЕРВИРОВАНИЕ данных.

С целью сохранения возможности восстановления файлов располагавшихся в начале диска желательно сделать резервную копию начальных секторов диска, подвергающимся изменениям в процессе восстановления.

В DiskEditor-е выделите режим просмотра первых 500-1000 физических секторов диска и сохраните их в виде файла на резервном диске. Более точный размер можно определить как сумму секторов: MBR трека + BR + 2FAT + ROOT + разумный резерв.

Возьмите дискету с зарегистрированной программой TIRAMISU, соответствующую типу файловой структуры восстанавливаемого диска. Руководствуясь инструкцией к этой программе, выполните предварительное восстановление данных на резервный диск.

Следует иметь в виду, что данная программа не затрагивает УбольнойФ диск, т.е. не правит на нем никакие данные. При некоторых особенностях УмусораФ в системных областях диска отмечены случаи сбоя программы TIRAMISU, что исправляется очисткой (обнулением) ошибочных данных (см. ниже).

3. ВОССТАНОВЛЕНИЕ Partition Table.

При восстановлении PT необходимо учитывать объем диска и особенности файловых систем диска FAT16 или FAT32.

Не пытайтесь создавать какой-либо раздел на диске с помощью программы Fdisk. При сканировании доступного дискового пространства fdisk прописывает в первый сектор на каждом треке код F6, что приводит к потере информации в этих секторах.

3.1. Если первый цилиндр (0/0/1) заполнен УмусоромФ - обнулите его (заполните нулями) для снижения возможных ошибок при восстановлении. Обнуление можно выполнить DiskEditor-ом.

3.2. Если Вы не знаете точно количество и размеры существовавших разделов диска или заведомо знаете о наличии дополнительного раздела диска, но не знаете размер основного раздела восстановите их, используя следующий способ: DiskEditor-ом скопируйте MBR и PT (сектор 0/0/1) с любого исправного диска на восстанавливаемый диск. Затем, очистив все записи кроме первой, отредактируйте ее, внеся заведомо искаженную информацию о конечном размещении раздела (например: 9999-й цилиндр) и общем количестве секторов (например: 99999999).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Начало размещения | | | Конец размещения | | | Смешение | Количество |
| Систем | Загр | Стор | Цилиндр | Сектор | Стор | Цилиндр | Сектор | Секторов | Секторов |
| BIGDOS | Да | 1 | 0 | 1 | 999 | 999 | 63 | 9999999 | 999999999 |

Запустив DiskDoctor, начните проверку восстанавливаемого диска, и на утверждение о найденных ошибках в PT и запросе на их устранение ответьте согласием. После внесения исправлений в искусственно созданную Вами PT, DiskDoctor предложит поиск возможных дополнительных DOS разделов. Естественно дайте на это согласие и если данные на диске в необходимом месте не повреждены - дополнительный раздел будет найден и после Вашего подтверждения восстановлен.

Как правило, после перезагрузки компьютера, данные дополнительного раздела становятся полностью доступными без дополнительных восстановительных операций. Учтите, что файлы возможно заражены вирусом.

Если Вы все проделали правильно, без ошибок и характер дисковых ошибок оказался не фатальным - первая задача выполнена, т.е. PT восстановлена.

3.4. Если вы уверены в существовании дополнительного раздела диска или какого-либо NON-DOS раздела (NTFS, Linux, ...), но NDD не смог его восстановить остаются еще способы ручного поиска.

3.4.1. Воспользуйтесь DiskEditor-ом (от PhysTechSoft), позволяющем осуществлять поиск различных NON-DOS разделов. И в случае нахождения подобных разделов на основании полученных номеров физических секторов вручную внесите информацию в PT.

3.4.2. Можно воспользоваться поиском PT в файлах резервирования. Различные системные программы типа менеджеров загрузки, утилит резервного сохранения и т.п. (о существовании которых пользователь иногда и не подозревает) выполняют операцию сохранения различной системной информации в файл. Воспользовавшись этим предположением, можно задать DiskEditor-у в режиме доступа к секторам физического диска маску поиска PT (55AAh или иную уникальную запись) и если повезет найти информацию о нем.

4. Восстановление BR, FAT и ROOT.

4.1. Восстановление BR, копий FAT и ROOT проще выполнить УавтоматическимФ способом, но это не исключает возможность УручногоФ восстановления с помощью карандаша, бумаги и редактора дисков. Как уже упоминалось выше, если на восстанавливаемом диске есть неповрежденные (или хотя бы частично поврежденные) элементы логической структуры сохраните их в виде файлов на резервном диске.

4.2. Выполните стандартное форматирование основного раздела диска, т.е. командой format С:. При этом формируется файловая структура форматируемого раздела диска с воссозданием BR, чистых FAT и ROOT, область данных при этом не затрагивается, т.е. информация в DA не изменяется.

4.3. Проверьте правильность местоположения корневой директории ROOT. Для этого DiskEditor-ом в режиме просмотра кластеров вновь созданного раздела, задав поиск объекта УПодкаталогФ, проверьте совпадение номеров физического кластера и номера кластера в первой записи найденных подкаталогов. В случае несовпадения номеров, необходимо подкорректировать значение числа секторов FAT в загрузочной записи BR. Корректировка осуществляется увеличением секторов на число кратное половине числа секторов в кластере. Как правило, такая корректировка необходима в случаях нестандартной разбивки диска или после изменений размеров разделов искусственным путем.

4.4. Если Вам повезло, и у Вас имеются зарезервированные в виде файлов уцелевшие образы FAT и/или ROOT следует, воспользовавшись DiskEditor-ом восстановить их на диске. Если у Вас уцелела вторая копия FAT, а первая нет, следует скопировать вторую копию и на место первой копии.

Если у Вас уцелела одна из копий FAT и корневой каталог ROOT, после выполнения всех пунктов 4.1 Ц 4.4 полноценный доступ к информации на диске будет восстановлен.

5. Восстановление DA (области данных).

При восстановлении данных следует иметь в виду, что, не имея достоверной информации в таблице расположения файлов (FAT) автоматическое или полуавтоматическое восстановление файлов размером более одного кластера программами типа UnFormat носит чисто случайный характер.

Упрощенно говоря, алгоритм восстановления данных подобными программами основан на поиске кластеров раздела диска с информацией о подкаталогах, анализе их содержания на предмет определения места расположения каталогов, определения номеров начальных кластеров каждого файла и анализе даты создания или стирания файлов. На базе этой информации строится дерево каталогов на логическом диске и расположение файлов по подкаталогам. Эта информация восстановима с большой степенью точности. В случае разрушения корневого каталога (ROOT) информация и файлах в корневом каталоге не восстанавливается, а имена директорий заменяются условными именами (типа DIR001).

Содержимое файлов имеющих размер более одного кластера восстанавливается с большой долей случайности, путем стыковки свободных последовательно расположенных кластеров, и вследствие больших объемов информации и интенсивной работы по созданию/удалению файлов в среде Windows (и не только) чаще всего некорректно.

Для точного восстановления информации необходимо либо восстановить FAT, либо осуществлять восстановление УвручнуюФ поиском и анализом содержимого кластеров на диске с дальнейшей стыковкой кластеров в необходимом порядке. Ручной способ в этом документе рассматриваться не будет.

Для попытки хотя бы частичного восстановления FAT можно воспользоваться особенностью работы ОС Windows 9x с виртуальной памятью, т.е. наличием на диске своп-файла. В этом файле могут находиться куски корневой директории ROOT и отдельные фрагменты, а подчас и полные копии FAT. Поиск этих фрагментов осуществляется в режиме просмотра секторов диска по уникальным маскам.

В качестве начальной маски поиска FAT может быть применен идентификатор F8 FF FF FF. В дальнейший поиск можно осуществлять по произвольным группам, состоящим из пяти последовательных 16-ти или 32-ти разрядных (FAT16 или FAT32) номеров кластеров, которые могут принадлежать какому-либо файлу. Поиск занимает довольно продолжительное время, но, меняя маски поиска, его стоит повторить несколько раз. Следует иметь в виду, что информация в своп-файле чаще всего располагается со смещением от начала секторов, что требует определенной коррекции при просмотре и дальнейшем применении. Основная задача отыскать максимальное число фрагментов, выбрать из них наиболее УсвежиеФ и составить из них подобие полной копии FAT. После проведения подобной операции возможно применение утилит типа UnErase для более полного (но возможно некорректного) восстановления файлов и DiskDoctor для коррекции дисковых ошибок.

Удачи, терпения и везения Вам!

ВНИМАНИЕ! Если информация на жестком диске УжизненноФ необходима, а Вы не уверены в своих знаниях и/или не исключаете возможной ошибки в своих действиях, не предпринимайте сами никаких восстанавливающих действий. Даже незначительная неточность в Ваших действиях может значительно осложнить или даже сделать невозможным дальнейшее восстановление информации.

СОВЕТ тем, кто САМ не сможет справиться с навалившейся на него проблемой. Обратитесь за помощью в технический центр к специалистам, которые возьмутся за решение Вашей проблемы.