платформах, а обмежений набір застосовуваних операцій дозволяє сподіватися на ефективну апаратну реалізацію.

Список літератури

1. *Вильям Столлингс*. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Издательский дом "Вильямс", 2001. – 672с.

2. *Петров А.А.* Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448с.

3. *Joan Daemen, Vincent Rijmen*. The Rijndael Block Cipher. AES Proposal: Rijndael, Document version 2, 3.09.99.

4. *Гулак Г.М., Горбенко И.Д., Михайленко М.С., Гитис Ю.Є.* Блочний симетричний криптоалгоритм SHACAL-2 // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", випуск – 7, 2003 р, 224 с.

Надійшла 13.10.2004р.

УДК 681.3.06(075)

С.Р.Коженевский

ОСОБЕННОСТИ ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ, ХРАНИМОЙ НА ЖЕСТКИХ ДИСКАХ

В компьютерных системах наиболее ценная и важная информация хранится в накопителях на жестких магнитных дисках (НЖМД). Это обуславливается их технико-экономическими показателями, такими как: энергонезависимость, простота в использовании, большие объемы данных при низкой стоимости хранения единицы информации, высокая скорость записи и считывания. Поэтому потеря данных, хранящихся на НЖМД, всегда очень болезненна для пользователей.

Широкому применению накопителей на жестких дисках способствует ряд его положительных эксплуатационных качеств: надежность, быстрота доступа и дешевизна в расчете на единицу хранения информации. Кроме того, один из самых важных показателей - энергонезависимость делает НЖМД практически незаменимым для оперативного и долговременного хранения больших массивов информации.

В то же время, размещение и хранение информации в устройствах долговременной энергонезависимой памяти создает предпосылки как для утраты важной информации, так и для несанкционированного доступа к ней.

Потеря информации на НЖМД может происходить вследствие износа рабочих поверхностей пластин жесткого диска, что приводит к нарушению служебных областей диска и области данных, либо вследствие его поломки. Кроме того, потеря данных может произойти и на полностью исправном НЖМД вследствие некомпетентных действий пользователей, системных сбоев, воздействий вирусов. Во всех этих случаях результат один - невозможность считывания информации штатными средствами.

Ценность утерянной информации изменяется в широких пределах: от малоценной до бесценной. В ряде случаев ценность утерянной информации настолько велика, что заказчик готов платить любые деньги за ее восстановление.

В последнее время значительно увеличился объем жестких дисков. В основном увеличение объема достигнуто за счет увеличения плотности записи. Увеличение плотности записи привело к необходимости применения специальных мер, направленных на увеличение надежности жестких дисков. Несмотря на принимаемые производителями жестких дисков меры по обеспечению надежности, жесткий диск остается самым ненадежным элементом компьютера. Ежегодно в сервисный центр «ЕПОС» поступает для ремонта более полутора - двух тысяч жестких дисков. Примерно треть из них имели

неисправности, обусловленные естественными причинами. Но две трети всех поломок обусловлены небрежным обращением с дисками. Поломка винчестера может привести к утрате важной информации. Для уменьшения риска утраты информации в серверах необходимо применять отказоустойчивые дисковые системы - RAID. Однако, применение таких систем может быть неприемлемо, например, по экономическим соображениям. Более того, утрата информации возможна и на исправном жестком диске, например вследствие случайного ее уничтожения или вследствие вирусной атаки. К счастью, в большинстве случаев информация теряется не безвозвратно. Ее можно восстановить.

В простейших случаях случайно уничтоженную информацию можно восстановить с помощью стандартных, широко распространенных утилит. Разработанные фирмой ЕПОС технологическая оснастка и специальные утилиты восстановления позволяют восстановить информацию в большинстве случаев и при поломке диска (в том числе, например, даже при обрыве головок).

Возможность восстановления информации основана на том, что при стирании информации средствами операционной системы фактически стираются только данные о расположении информации на диске, а сама информация физически не уничтожается. Поэтому задача восстановления информации в большинстве случаев сводится к решению трудной, но выполнимой логической задачи. Даже уничтожение загрузочного сектора (так, например, поступает вирус «CIH») не является серьезным препятствием для восстановления данных, так как конкретные значения блока параметров BIOS (размер кластера, число кластеров в томе, число элементов FAT и т.п.) может быть получено расчетным путем.

Уничтожение таблиц FAT (например, при форматировании диска) значительно усложняет задачу восстановления данных, т.к. именно они являются жизненно важными схемами расположения файлов. Вся область файлов становится морем информации без каких-либо указателей. Автоматическое восстановление данных с помощью утилит не гарантирует полного восстановления, и чем больше степень фрагментации файлов, тем меньше вероятность их восстановления. Полное восстановление возможно только в интерактивном режиме специалистами по восстановлению информации, но это уже требует применения специализированного программного обеспечения и значительных временных затрат.

Механические повреждения элементов, расположенных в камере винчестера, как правило, исправить уже нельзя. Тем не менее, если, например, оборвалась магнитная головка, то в нашем сервисном центре смогут восстановить информацию. Для этого специалисты вскроют камеру, установят новую магнитную головку и восстановят потерянные данные.

Восстановление информации применяется не только с целью восстановления утраченной информации, но и в целях разведки: путем восстановления конфиденциальной информации, например, на дисках, возвращенных по гарантии или сданных в утиль. Ввиду невозможности, в большинстве случаев, произвести ремонт и обслуживание вышедшего из строя НЖМД на месте производят его замену на новый. При этом вся информация в доступном или недоступном для операционной системы виде остается на подлежащем замене НЖМД.

В ряде случаев злоумышленники применяют принцип имитации выхода компьютеров из строя по вине НЖМД после определенного периода функционирования и накопления информации. Так как договор гарантии, как правило, распространяется на всю партию компьютерной техники и предусматривает замену НЖМД на безоплатной основе при сохранности пломб и соблюдении правил эксплуатации, то сервисному центру или организации, обеспечивающим поставку компьютерной техники, добровольно передается информация, хранящаяся на НЖМД.

Для предотвращения утечки информации в простейшем случае возможна запись произвольных данных в файл, ранее содержащий конфиденциальную информацию. В этом случае невозможно восстановление информации средствами широко распространенных утилит. Однако, утилиты специального назначения могут во многих случаях восстановить данные в

поврежденных секторах диска путем, например, статистического накопления информации при многократном считывании данных в поврежденных секторах. Данный метод применяется, в частности, в приборах и утилитах, разработанных фирмой ЕПОС для копирования информации с дисков, имеющих незначительные повреждения поверхности. Поэтому, необходимо для уничтожения информации записывать случайные данные не только в те сектора жесткого диска, в которых хранилась важная информация, а во все сектора, включая и поврежденные. Как правило, это осуществимо только с помощью узкоспециализированного программного обеспечения или с помощью специальной аппаратуры. В последнее время разработаны более мощные методы восстановления информации, в частности, основанные на принципах магнитной силовой микроскопии (MFM). MFM основана на сканирующей зондовой микроскопии.

Возможность восстановления информации на НЖМД основывается на следующих факторах:

- Изменениях чувствительности головок и напряженности магнитного поля на поверхности пластины во времени.
- Невозможности точного позиционирования головки записи в каждом процессе записи.

В обоих этих случаях головка записи изменяет полярность большинства, но не всех магнитных областей (доменов). Если для работы берется новый жесткий диск, то при первой записи данных на его рабочую поверхность при записи 1 записывается 1, при записи 0 - записывается 0. Однако при перезаписи 1 поверх 0 фактически запишется величина по амплитуде равная 0,95, а при перезаписи 1 поверх 1 величина поля по амплитуде будет составлять 1,05 [1]. Обычный контроллер жесткого диска будет считывать эти значения как равные 1, но при использовании специализированных устройств действительные состояния могут быть детектированы. Восстановление одного или двух «слоев» записанных данных несложно осуществить, считав данные специальной аналоговой головкой с высококачественным осциллографом и затем проанализировав сигналы с помощью специализированного программного обеспечения (ПО). Такое ПО генерирует «идеальный» сигнал считывания и вычитает из него действительный сигнал. В результате получается остаток предыдущего сигнала.

Методы восстановления данных, сохраненных на магнитных накопителях, стали бурно развиваться с изобретением методов магнитной силовой микроскопии (MFM), основанной на сканирующей зондовой микроскопии (SPM).

Для построения изображения образца SPM микроскопы используют острый наконечник. Между ним и образцом подается напряжение смещения. При сближении наконечника и образца на расстояние d ~ 10E электроны из образца начинают туннелировать в наконечник.

Возникающий туннельный ток изменяется в зависимости от расстояния между наконечником и образцом. Этот ток и является выходным информационным сигналом. Зонд сканирует анализируемую поверхность на расстоянии порядка 10 -100 Е, при этом система обратной связи непрерывно корректирует его положение в вертикальной плоскости с помощью оптического интерферометра или туннельного зонда [1]. После сканирования наконечником поверхности образца строится его изображение. Однако методы SPM микроскопии не позволяют получить изображение пространственного распределения магнитного поля. Для этого применяют метод MFM.

Взаимодействие наконечника с магнитным полем анализируемой поверхности изменяет частоту колебания консоли. Этот сдвиг частоты детектируется с помощью оптического интерферометра. На основании полученных данных формируется изображение зон намагниченности.

Если автоматизировать последовательность сбора данных об участках диска и обеспечить сбор информации со всего диска для создания его электронного образа, то задача восстановления информации будет решена. Соответствующее программное обеспечение (ПО) и специализированный компьютер теоретически могут решить данную задачу.

По данным изготовителей, в настоящее время эксплуатируется несколько тысяч SPM микроскопов, причем многие из них производились для анализа поверхностей пластин жестких дисков.

Существуют также и другие методы анализа магнитных сред. Суть их заключается в использовании ферромагнитных жидкостей или тонких ферромагнитных пленок в комбинации с оптическими микроскопами. Физический принцип регистрации статического магнитного поля следующий. Магнитное поле исследуемой поверхности воздействует на структуру магнитооптического кристалла. В результате быстрого нагревания кристалла до «точки Кюри» в нем фиксируется «отпечаток» исследуемого магнитного поля, который можно увидеть и зафиксировать через оптический микроскоп. Недостатком такого метода является его неэффективность при плотностях записи порядка Гбит/кв.дюйм, поскольку в этом случае размер магнитных доменов меньше длины волны видимого света [2].

Сформулируем какие же факторы влияют на эффективность восстановления информации:

1. Изменение температуры.

Зависимость коэрцитивной силы от температуры также влияет на возможность перезаписи. Если данные первоначально были записаны при температуре, при которой коэрцитивная сила была низка, а перезаписаны, при которой коэрцитивная сила относительно высока, то сохраняется потенциальная возможность восстановления первоначальных данных. Это важно для жестких дисков, температура внутри корпуса которых колеблется.

Эффективность перезаписи зависит и от температурных изменений в головке записи/чтения.

2. Старение.

Старение также оказывает влияние на стираемость магнитных накопителей. Отмечено снижение стираемости на несколько дБ, причем стираемость данных зависит не от возраста магнитного носителя, а от времени хранения данных в магнитном носителе.

На основании проведенных исследований можно отметить следующие дополнительные методы восстановления информации, хранимой на НЖМД:

1. Использование дефектных секторов.

После изготовления HDD магнитная поверхность диска сканируется на наличие дефектов, которые записываются в карту дефектов. Появляющиеся в процессе эксплуатации дефекты добавляются в эту карту аппаратным или программным обеспечением контроллера НЖМД.

Существует несколько методов маскировки дефектов поверхности в процессе работы HDD:

- перенос данных на резервную дорожку, размещаемую между дорожками данных. При этом значительно уменьшается полезная емкость накопителя;
- размещение резервных секторов в конце каждой дорожки. В эти сектора переносят данные с поврежденных секторов на дорожке. Это уменьшает емкость накопителя на 1 3%. При этом методе увеличивается и время ожидания;
- встроенный резервный сектор. Используется размещение резервного сектора в конце каждой дорожки. При обнаружении дефектного сектора переназначаются идентификаторы секторов так, что дефектный сектор пропускается, и запись/считывание осуществляется из резервного сектора в конце дорожки. Это самый эффективный метод, так как вносимая задержка равна времени, необходимому, чтобы пропустить дефектный сектор.

При удалении данных с HDD программным путем, как правило, забывают о наличии дефектных секторов, куда когда-то была записана информация. Диск со временем стареет и количество информации, сохраненной в дефектных секторах, растет. Эти данные могут быть считаны и оказаться очень полезными при восстановлении информации на диске.

2. Использование корректирующих кодов.

Увеличение плотности записи вызывает появление ошибок чтения данных, и производители HDD стали применять сложные корректирующие коды, исправляющие пакеты многократных ошибок. Типичный привод может иметь в каждом секторе 512 байт данных, 4 байта CRC и 11 байт корректирующего кода (ECC). Такой корректирующий код способен исправлять одиночные пакетные ошибки длиной до 22 бит, двойные пакетные ошибки длиной до 11 бит и обнаруживать одиночные пакетные ошибки длиной до 51 бит [1].

Поэтому, даже если некоторые данные гарантировано удалены, существует теоретическая возможность их восстановления, используя возможности коррекции ошибок.

Выводы

С развитием методов записи информации на HDD развиваются и методы восстановления потерянных (удаленных) данных. Поэтому актуальной задачей является осознание особенностей хранения важных данных на HDD, резервирования их, а также осознание надежного удаления их с магнитного носителя.

Список литературы

1. Gutmann, Peter. Secure Deletion of Data from Magnetic and Solid-State Memory. University of Auckland, 1996.

2. Upgrading and repairing PCs. Tenth Anniversary Edition. Scott Mueller, Craig Zacker. Que Corporation, 1998.

Поступила 1.11.2004г.

УДК 681.3.06

Головань С.М., Давиденко А.М., Мелешко О.О.,
Щербак Л.М., Щербина В.П.

СТВОРЕННЯ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Вступ

На сьогодні впровадження інформаційних технологій, інформаційно-аналітичних систем і інформаційних систем, управління у різні галузі народного господарства України є важливою і актуальною науково-технічною проблемою. У 2003 році прийняті закони „Про електронні документи та електронний документообіг", „Про електронний цифровий підпис". Введено в дію ряд інших директивних документів, в тому числі стандарт ДСТУ 4145-2002 на електронний цифровий підпис [1...3]. В даній роботі розглянуті основні проблеми створення системи електронного документообігу, які також є актуальними та важливою складовою комплексного вирішення державних науково-технічних проблем. Застосування механічних і електричних друкарських машинок, на сьогодні інформаційні (автоматизовані) системи (організаційно-технічна система, що реалізує інформаційну технологію і об'єднує обчислювальну систему, фізичне середовище, персонал і інформацію, яка обробляється) стали відповідними етапами розвитку систем документообігу.

Прийнято вживати два поняття – діловодство та документообіг. Відмітимо, що поняття діловодство (цей термін з'явився в другій половині XVIII ст.) позначало діяльність, якою займалась не тільки і не стільки канцелярія, скільки весь апарат підприємства, установи, організації в цілому. Термін „діловодство" походить від словосполучення слів „ведення діл", а під „ділом" в той час розумілась не папка з документами, як в сучасному значенні цього слова, а розгляд і вирішення питання, „ведення діл" (виробництво справ) – це не що інше, як вирішення справи. Оскільки всяке вирішення передбачає його письмову фіксацію на всіх стадіях, то природно, діловодство розумілось і як „правила, якими канцелярія керувалась в складанні доповідних записок, ведення журналів обліку паперів, визначень та актів взагалі, і виконання паперів". В свою чергу документообіг – переміщення