захисту інформації в Україні. НТУУ „КПІ”. – 2002. – №. 3. – С. 10-24. 6. Антонюк А. Жора В. Загрози інформації і канали витоку. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, науково-технічний збірник, вип. 2, НТУУ „КПІ”. К. 2001 р. 7. Метод захисту цілісності інформації, яка передається в системах абонентського радіодоступу спеціального призначення / Корнейко О. В., Кувшинов О. В., Лівенцев С. П. // Збірник „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. НТУУ „КПІ”. – 2002. – №. 4. – С. 60-66. 8. Банкет В. Л., Дорофеев В. М. Цифровые методы в спутниковой связи. – М.: Радио и связь, 1988. – 240 с. 9. Зяблов В. В., Коробков Д. Л., Портной С. Л. Высокоскоростная передача сообщений в реальных каналах. – М.: Радио и связь, 1991. – 288 с.

УДК 621.96

ОСОБЕННОСТИ ХРАНЕНИЯ, ВОССТАНОВЛЕНИЯ И УНИЧТОЖЕНИЯ ИНФОРМАЦИИ НА ЖЕСТКИХ ДИСКАХ

Сергей Коженевский
ООО «ЭПОС»

Аннотация: **Обобщается опыт фирмы ЕПОС по ремонту жестких дисков и восстановлению информации, приводятся специфические каналы утечки информации, хранящейся на жестких дисках, описывается принцип построения стенда технического обслуживания жестких дисков с возможностью гарантированного уничтожения информации.**

Summary: **In this paper the experience of EPOS company in hard drives repair and data recovery is summarized. The specific channels of leakage of data stored on hard drives are considered. In this paper also are described the structure of hard drives maintenance test bench with provision of secure data erasure.**

Ключевые слова: **Информация, информационная безопасность, техническая защита информации.**

В информационных системах, базовым элементом которых является компьютер, основные объёмы информации хранятся на жёстких магнитных дисках.

Именно в накопителе на жестких магнитных дисках (НЖМД) хранится и с него загружается в оперативную память компьютера его операционная система, информация, обрабатываемая в процессе использования, а также использованная и удаляемая информация.

Широкому применению НЖМД способствует ряд их положительных эксплуатационных качеств: надежность, быстрота доступа и дешевизна (в расчёте 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 создаёт предпосылки как для утраты важной информации, так и для несанкционированного доступа к ней.

В последнее время значительно увеличился объем информации, хранимой на жестких дисках. 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 серьёзным 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 расчётным 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. Вскрытие камеры жесткого диска осуществляется в специально оборудованной «чистой комнате». «Чистая комната» – сложное инженерное сооружение. Она устроена как матрешка: отдельная изолированная от остальных помещений комната, в которую подается чистый воздух от кондиционера. Внутри этой комнаты расположена еще одна комната, в которой оборудованы два контура очистки воздуха. Внутри этой комнаты расположено собственно рабочее место, оборудованное дополнительной системой очистки воздуха (рис. 1).

Рисунок 1 – Слева – рабочее место по ремонту дисков в чистой комнате, справа – прецизионная установка для замены головок

Тем не менее, в случае механических повреждений элементов, расположенных в камере жесткого диска, можно говорить только о восстановлении информации, но не о дальнейшей эксплуатации диска.

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 остаётся на подлежащем замене НЖМД.

В ряде случаев злоумышленники применяют принцип имитации выхода компьютеров из строя по вине НЖМД после определённого 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 передаётся 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.

Магнитный наконечник зонда движется над поверхностью пластины на расстоянии порядка 10 - 100 Å. В зависимости от силы магнитного взаимодействия между пластиной и наконечником расстояние между ними изменяется. Эти колебания расстояния детектируются оптическим интерферометром. Полученное изображение представляет собой образ распределения намагниченности.

Этими методами можно измерить магнитный рельеф поверхности диска и, следовательно, восстановить информацию.

Важно отметить, что вследствие очень высокой плотности записи механическая система (привод магнитной головки) не в состоянии точно следовать по требуемой траектории. Поэтому при записи новых данных поверх конфиденциальной информации новые данные всегда будут записаны с некоторым смещением относительно ранее записанных данных (рис. 2).

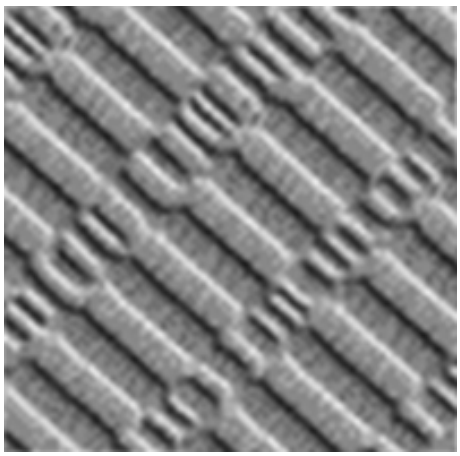

Рисунок 2 – Магнитный рельеф поверхности жесткого диска, полученный с помощью MFM

Разрешающая способность магнитной силовой микроскопии достаточна для раздельного считывания нескольких последовательных записей информации.

Для гарантированного уничтожения конфиденциальной информации разработаны различные методы, которые условно можно разделить на две большие группы:

- уничтожение данных с сохранением работоспособности накопителя;
- уничтожение данных с потерей работоспособности накопителя.

При гарантированном уничтожении информации с сохранением работоспособности накопителя, как правило, осуществляется многократная запись в каждый сектор жесткого диска специально подобранных кодов. Запись специальных кодов осуществляется также в поврежденные и резервные сектора. Гарантированное уничтожение данных с сохранением работоспособности накопителя осуществляется, как правило, аппаратными средствами, хотя в некоторых случаях применимы и программные средства.

Известно несколько алгоритмов, применение которых обеспечивает гарантированное уничтожение информации с определенной достоверностью (табл. 1)

Таблица 1 – Сравнительная характеристика алгоритмов уничтожения информации

Алгоритм	Содержание алгоритма
Руководство по защите информации МО США (NISPOM) DoD 5220.22-M, 1995 г.	Количество циклов записи – 3. Цикл 1 – запись произвольного кода. Цикл 2 – запись дополнения к нему. Цикл 3 – запись случайных кодов.
Стандарт VISR, 1999 г. (Германия)	Количество циклов записи – 3. Цикл 1 – запись нулей. Цикл 2 – запись единиц. Цикл 3 – запись кода с чередованием нулей и единиц.
ГОСТ Р50739-95 г. (Россия)	Количество циклов записи – 2. Цикл 1 – запись нулей. Цикл 2 – запись случайных кодов.
Алгоритм Брюса Шнейера	Количество циклов записи – 7. Цикл 1 – запись единиц. Цикл 2 – запись нулей. Циклы 3..7 – запись случайных кодов
Алгоритм Питера Гутманна	Количество циклов – 35. Циклы 1..4 – запись произвольного кода. Циклы 5..9 – запись специальных комбинаций Циклы 10..25 – последовательная запись комбинаций от 00 до FFh. Циклы 26.. 31 – аналогично циклам 5..9 Циклы 32..35 – аналогично циклам 1..4.

Наиболее часто употребляются алгоритмы, определенные в стандартах России и США. Для современных накопителей с очень высокой плотностью записи уже при двух–трех циклах записи стоимость восстановления информации становится неприемлемо высокой. Тем не менее, в коммерческих системах стремятся для надежности применять алгоритм Гутманна, хотя время уничтожения информации при этом увеличивается в десятки раз.

Сущность способов гарантированного уничтожения данных с потерей работоспособности накопителя заключается в таком воздействии на рабочие слои дисков, при котором разрушается физическая, химическая либо магнитная структура рабочего слоя. К таким способам можно отнести: механическое разрушение дисков (прессование, механическое эрозирование поверхности – пескоструй, ультразвуковое и электрохимическое эрозирование), химическое травление в агрессивных средах и обжиг или переплавку дисков. Съём данных с магнитных дисков, подвергшихся таким воздействиям, становится невозможным ни практически, ни теоретически. Естественно, при этом дальнейшее использование накопителя уже невозможно.

К группе способов гарантированного уничтожения данных с потерей работоспособности накопителя относится и воздействие на диски мощным постоянным или переменным магнитным полем, при котором разрушается магнитная структура рабочих поверхностей, в том числе служебная информация низкоуровневого форматирования и сервометки. У современных накопителей на жестких дисках низкоуровневое форматирование и нанесение магнитных сервометок осуществляется только на заводе–изготовителе. После уничтожения сервометок их восстановление практически невозможно. Более того, сервометки записываются значительно более мощным магнитным полем, чем во время эксплуатации осуществляется запись информации. Поэтому если в результате воздействия магнитного поля уничтожены магнитные сервометки, то записанную в процессе эксплуатации информацию тем более невозможно будет восстановить. Дальнейшая эксплуатация накопителя после воздействия мощного магнитного поля также невозможна, но накопитель при этом физически остается не поврежденным и может быть, например, заменен по гарантии.

Оба рассмотренных способа обеспечивают достаточный уровень гарантии уничтожения информации. Более практичным считается способ с сохранением работоспособности накопителя. Во-первых, накопители после уничтожения данных могут эксплуатироваться и в дальнейшем. Во-вторых, способы уничтожения определены стандартами, что вызывает определенный уровень доверия. Однако, чаще всего выход накопителя из строя для пользователя является неожиданным и происходит в самый неподходящий момент. Поэтому зачастую пользователь не может самостоятельно уничтожить информацию, хранившуюся на

ставшем неисправным НЖМД. Более того, при неисправности элементов, расположенных в камере накопителя даже в условиях специализированного сервисного центра невозможно гарантировать, что в процессе ремонта сохранится исходное расположение головок. Поэтому за исключением простейших случаев (отказ контроллера диска) при выходе накопителя из строя гарантированно уничтожить информацию можно только разрушающими методами.

Опыт фирмы ЕПОС по ремонту жестких дисков и восстановлению информации позволил создать стенд для технического обслуживания жестких дисков (рис. 3).

Рисунок 3 – Стенд для технического обслуживания жестких дисков

Стенд позволяет осуществить полную диагностику жесткого диска, адаптивное копирование дисков (даже при некоторых повреждениях диска – источника), а также гарантированное уничтожение информации путем многократной записи специальных кодов во все физические сектора жесткого диска.

В настоящее время в ООО «ЭПОС» проводится ОКР по подготовке к серийному производству следующего поколения стенда для технического обслуживания накопителей на жестких дисках, имеющего расширенные функции как по диагностике накопителя, так и по уничтожению информации. В частности, для уничтожения информации на дисках, имеющих значительные повреждения, стенд комплектуется устройством, позволяющим стирать данные на всем диске, включая служебные области и сервометки, путем воздействия мощного магнитного импульса.

УДК 681.3.06

ЗАЩИТА ДАННЫХ НА КОМПАКТ-ДИСКАХ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

Виталий Носов, Александр Манжай

Национальный университет внутренних дел, г. Харьков

Анотація: **Проведено аналіз відомих принципів захисту даних на компакт-дисках від несанкціонованого копіювання. Розглянуто новий метод, що забезпечує більш високий ступінь захисту від копіювання.**

Summary: **The analysis of known principles of the data protection on compact discs from the non-authorized copying is carried out. The new method providing the big degree of protection against copying is considered.**

Ключевые слова: **Защита данных, несанкционированное копирование, компакт-диск.**

I Введение

В условиях стремительного развития компьютерной техники остро встала проблема защиты интеллектуальной собственности, носителем которой, прежде всего, являются компакт-диски (CD). В настоящее время со стороны компаний-производителей программного обеспечения и мультимедийных CD активизирована борьба с незаконным копированием и тиражированием таких компакт-дисков. Однако эффективных результатов она пока не приносит, что связано с необходимостью постоянного поиска новых и совершенствования существующих методов защиты компакт-дисков от несанкционированного копирования.

В общем случае система защиты CD представляет собой комплекс средств, предназначенный для затруднения (в идеале – предотвращения) нелегального копирования (исполнения) защищаемого программного модуля, с которым она ассоциирована.

В настоящее время уже устоявшейся можно считать структуру системы защиты CD, которая