14. *M.Blum, S.Micali*. How to generate cryptographically strong sequences of pseudo-random bits// SIAM J. Comput., vol.13, no.4, 1984, pp.850-864.

15. Randomness Recommendations for Security. *D.Eastlake*, 3rd DEC *S.Crocker* Cybercash, *J.Schiller* MIT, December 1994.

16. *Кнут Д.* Искусство программирования для ЭВМ: В 3-х т. Получисленные алгоритмы. Пер. с англ. – М.: Мир, 1977. – Т.2. – 724 с.

17. Hardware-based Random Number Generation, An RSA Data Security While Paper, RSA Data Security, Inc, 1999.

Надійшла 4.02.2003р.

УДК 681.324

Коженевский Р.С.

МЕТОДЫ ГАРАНТИРОВАННОГО УНИЧТОЖЕНИЯ ДАННЫХ НА НАКОПИТЕЛЯХ НА ЖЕСТКИХ МАГНИТНЫХ ДИСКАХ

За последние несколько десятилетий компьютерные информационные технологии прочно вошли в нашу жизнь и стали составной частью документооборота. Первоначально отработанные механизмы обеспечения информационной безопасности для новых компьютерных систем уже не подходят, и требуют существенной модернизации. В первую очередь это касается отношения к информации, хранящейся на накопителях на жестких магнитных дисках (НЖМД).

Ранее для снятия информации с НЖМД был необходим физический доступ к носителю. Появление же компьютерных сетей создало новые угрозы безопасности информации, так как позволяет дистанционно, а иногда и скрыто от пользователя, получить доступ к хранимой на компьютере информации.

В настоящее время на развитие индустрии защиты информации (ЗИ), тратятся миллионы долларов. А по сути дела, решается одна задача – сделать открытую информацию доступной всем пользователям, а конфиденциальную – доступной только тому, кому она предназначается. Как в сфере бизнеса, так и в сфере государственного управления, уже скопились значительные объемы конфиденциальной информации, хранящиеся в базах данных персональных компьютеров (ПК). Эта информация представляет собой реальную ценность, а утечка ее в ряде случаев способна влиять даже на государственную безопасность.

Данное обстоятельство дало мощный толчок к развитию всевозможных программных и аппаратных средств добывания информации из ПК и компьютерных сетей. Особенно уязвимыми оказались сети, имеющие прямой выход в интернет.

Пути или каналы утечки информации, позволяющие несанкционированно и безнаказанно снимать копии с информации, непосредственно связаны с технологиями обработки, передачи и утилизации информации, хранящейся на НЖМД [1].

Утечка информации при замене НЖМД

Быстрое устаревание компьютерных технологий это уже установившееся явление. Каждые два года (по закону Мура) ПК удваивают свою мощность. После смены двух поколений ПК не представляет собой никакой ценности и его нецелесообразно поддерживать технически и программно. Как правило, персональные компьютеры окупаются за 4 года, а это означает, что ИТ-компании должны заменять 25%

компьютерного парка в течение каждого года. Замена этих компьютеров может осуществляться разными способами:

1. Перенос ПК на другое место.

Часто замена ПК принимает форму переноса компьютера с места, изначально предназначенного для решения определенных задач, на рабочее место, требующее меньшей вычислительной мощности. После переустановки системы старый ПК можно будет использовать на новом месте как автоматизированную систему начального уровня. Переустановка системы не очищает НЖМД от ранее хранимой информации и вся или почти вся старая информация попадает к новому владельцу.

2. Продажа ПК как «second hand».

Даже если система не находит применения в организации, она может быть продана полностью или по частям учреждениям, которые могут использовать ее целиком или отдельные комплектующие (сервисные центры, начинающие пользователи и т.д.). Компании, представляющие повышенные требования к вычислительной мощности своих ПК, вынуждены почти каждый год продавать или модернизировать их, чтобы частично возместить свои инвестиции.

3. Дарение ПК.

Очень часто старые ПК безвозмездно передаются детским учреждениям или благотворительным организациям.

Во всех этих случаях старые ПК вместе с НЖМД вывозятся вместе со всеми данными, на защиту которых были потрачены деньги и время, и это происходит в крупных организациях почти каждый день.

В то время, как существуют не только законы, но и аппаратные средства, запрещающие или препятствующие получению конфиденциальной информации, снятие данных со списанного НЖМД позволяет заинтересованному лицу не только обойти системы безопасности без проявления внешних признаков, но и сделать это практически законно.

Многие руководители организаций и пользователи ПК не знают, что простое удаление файлов или даже переформатирование НЖМД фактически не удаляет данные. Стоит только однажды записать информацию на НЖМД и удалить ее из магнитной памяти диска будет очень сложно. Поэтому, казалось бы, безвредный акт списания старого компьютера или передача его в другую организацию – наиболее простой путь к информации с ограниченным доступом.

Кроме той конфиденциальной информации, о которой знают пользователи (бухгалтерской, финансовой, личной, перспективные разработки), на ПК может храниться множество других конфиденциальных данных, которые не всегда известны оператору.

Приложения и операционные системы (ОС) хранят пароли, ключи шифрования и другие данные с ограниченным доступом в различных местах, включая файлы конфигурации и временные файлы. Операционные системы произвольным образом записывают содержимое памяти в файл подкачки на диске, что не дает возможности узнать, что из этих данных действительно сохранено на носителе.

В настоящее время проблемой является и установленное программное обеспечение (ПО) персональных компьютеров. Практически все лицензионное ПО не может передаваться без лицензий со старым аппаратным обеспечением. Поэтому требование по удалению лицензионного ПО при продаже или передаче устаревшего ПК остается.

Утечка информации при замене неисправного НЖМД

Еще одним и очень важным каналом утечки информации является неисправный НЖМД.

По мнению Ontrack – компании-мирового лидера по восстановлению информации на неисправных НЖМД – в 78% случаев потери данных виноваты аппаратные сбои НЖМД (статистику компании ЕПОС по потере информации можно найти в [2]). Современные технологии хранения информации на магнитных носителях развиваются очень быстро. На современных НЖМД хранится в 500 раз больше информации, чем 10 лет назад. Значительно увеличилась плотность хранения информации и скорость вращения магнитных пластин, но, к сожалению, такой показатель, как надежность НЖМД, ухудшился. Так, практически все производители дисков перешли с 3-х годичной гарантии на одногодичную [3 – 6].

Большинство дисков ломаются в гарантийный период и должны быть заменены по гарантии при условии сохранности пломб и отсутствии механических повреждений или следов вскрытия. Считать информацию с диска, переписать ее на другой носитель или стереть не предоставляется возможным по причине неисправности НЖМД. В этом случае НЖМД с информацией обменивается фирмой-продавцом на новый накопитель, а неисправный накопитель отсылается производителю или переводится на длительное хранение. В большинстве случаев причина выхода НЖМД из строя – неисправность механики или контроллера, которые могут легко быть заменены или отремонтированы на заводе-производителе или в специализированном сервисном центре компьютерных систем, которые находятся за рубежом. Огромное количество информации, в том числе и конфиденциальной, попадает в руки лиц, доступ которых нежелателен. Даже если представить, что в гарантийный период выйдет из строя 10% НЖМД при количестве проданных в Украине в 2002г. – 500 000 шт. [7], то общий объем информации, уходящей за рубеж, в весовом выражении составит 25 тонн.

500 000×0,1×0,5кг = 25 000кг

Над этими цифрами стоит задуматься.

Основные положения защиты информации, хранимой на НЖМ, от несанкционированного доступа

Обеспечение надежного уничтожения корпоративной информации в конце жизненного цикла НЖМД требует тщательной проработки вопросов безопасности информации.

Удаление данных с НЖМД само по себе не обеспечивает защиты информации. Процесс ЗИ должен основываться на ряде согласованных методик, обеспечивающих в конечном итоге высокую вероятность уничтожения информации.

Хотя ни одна из методик не может гарантировать 100% надежность уничтожения информации [8], существуют основные положения и условия защиты информации:

1) Необходимость физической защиты НЖМД. Кража ПК или отдельных НЖМД приводит к утечке информации, поэтому необходимо обеспечить их физическую сохранность с момента окончания срока эксплуатации до получения документированного подтверждения об уничтожении данных.

2) Систематический контроль и ведение отчетности.

Систематический контроль подразумевает отслеживание выбывающих из эксплуатации НЖМД, контроль процесса уничтожения информации и составление отчета об отклонениях в этом процессе и допущенных ошибках. Необходимо фиксировать следующие сведения:

- уникальный идентификационный код уничтожаемого НЖМД;
- дата и время уничтожения;
- ФИО исполнителя;
- использованная методика уничтожения.

Таким образом, алгоритм обеспечения защиты информации (ЗИ), хранимой на НЖМД, от несанкционированного доступа должен включать следующие действия:

1) Физическая защита информации, включающая в себя инвентаризацию и ограничения доступа к НЖМД.

2) Систематический контроль над процессом замены, передачи и уничтожения информации на НЖМД.

3) Использование стандартизованных приложений и методик по уничтожению информации на НЖМД.

4) Систематическая проверка процессов уничтожения информации на НЖМД, включая носители.

5) Периодический контроль надежности уничтожения информации с произвольно выбранных НЖМД.

6) Выбор методик и способов для уничтожения информации на неисправных НЖМД, путем анализа категорийности хранимой на них информации.

7) Обеспечение процедуры сбора и уничтожения НЖМД.

8) Ведение отчетности по каждому уничтоженному НЖМД.

Способы уничтожения информации, хранимой на НЖМД

В настоящее время существует несколько способов уничтожения информации, хранимой на НЖМД. Уничтожение подразумевает стирание или удаление (очистку) информации с НЖМД таким образом, что ее невозможно восстановить ни обработкой на компьютерах с помощью специального ПО, ни с помощью лабораторных средств (например, изучение поверхностей магнитных пластин с помощью сканирующей микроскопии. [9]).

Способы уничтожения информации на НЖМД делятся на три большие группы [10]:

1) **Программные**, в основу которых положено уничтожение информации, записанной на магнитном носителе, посредством штатных средств записи информации на магнитных носителях. В случае уничтожения информации на НЖМД программным методом, он может быть повторно использован в других ПК, после инсталляции новой ОС и приложений. Уничтожение производится наиболее простым и естественным способом – перезаписью информации. Перезапись – это процесс записи несекретных данных в область памяти, где ранее содержались секретные данные.

Следует отметить очень важную деталь – при перезаписи информации работоспособность НЖМД полностью сохраняется, в случае, если он был полностью исправным. На изношенном или неисправном НЖМД провести надежное уничтожение информации невозможно.

2) **Механические**, связанные с механическим повреждением основы, на которую нанесен магнитный слой – физический носитель информации.

3) **Физические**, связанные с физическими принципами цифровой записи на магнитный носитель, и основанные на перестройке структуры магнитного материала рабочих поверхностей носителя.

По способу воздействия на устройство (НЖМД):

1) Без разрушения конструктива и поверхностей НЖМД.

2) С разрушением НЖМД.

Программные способы уничтожения информации на НЖМД

1) <u>Начальный уровень (уровень 0).</u>

Наиболее простая и часто применяемая форма уничтожения информации на НЖМД. Вместо полного стирания НЖМД в загрузочный сектор, основную и резервную таблицы разделов записывается последовательность нулей.

В этом случае данные на диске не уничтожаются, к ним усложняется доступ. Полный доступ к информации на НЖМД легко восстанавливается с помощью специального ПО, производящего анализ секторов диска (Norton DiskEdit, WinHex).

2) Уровень 1.

Производится запись последовательности нулей или единиц в сектора данных. При этом уничтожается не только загрузочная область, но и данные.

Обычным пользователям в этом случае практически невозможно восстановить уничтоженную информацию.

Тем не менее, существует возможность восстановления информации при стирании перезаписью. В основе ее лежат:

- ошибки оператора и неправильное использование ПО.
- отказ ПО перезаписывать все адресуемое пространство диска.
- остаточная информация в дефектных секторах.
- анализ зон остаточной намагниченности и эффекте краев дорожек.

Восстановить информацию, удаленную этим методом стандартными средствами невозможно. Для восстановления требуются специальные знания и оборудование [9, 11].

3) Уровень 1+.

Используются несколько циклов перезаписи информации.

Чем больше циклов перезаписи информации, тем сложнее восстановить удаленные данные. Это связано с неточностью позиционирования головки. Чем больше раз головка перезапишет данные, тем выше вероятность, что она сотрет зоны остаточной намагниченности на краях дорожки.

Последовательности, прописываемые в сектора данных, стандартизированы. Наиболее часто употребляемые сведены в табл. 1 - сравнительную таблицу алгоритмов уничтожения данных на накопителях с жесткими магнитными дисками методом перезаписи данных во всех адресуемых секторах.

Таблица 1. Сравнительная таблица алгоритмов уничтожения данных

Алгоритм	Содержание алгоритма	Примечания
Руководство по защите информации МО США (NISPO) DoD 5220.22-M, 1995г.	Количество циклов записи – 3. Цикл 1 - запись произвольного кода. Цикл 2 - запись инвертированного кода. Цикл 3 - запись случайных кодов.	NISPO запрещает использование этого алгоритма для уничтожения данных с грифом:"СОВ.СЕКРЕТНО" Альтернативные способы (в соответствии с NISPO): -размагничивание; -физическое разрушение
Стандарт VISR, 1999г. (Гемания)	Количество циклов записи – 3. Цикл 1 – запись нулей. Цикл 2 – запись единиц. Цикл 3 - запись кода с чередованием нулей и единиц.	

Продолжение таблицы 1

ГОСТ Р50739-95г. (Россия)	Для классов защиты данных 1..3 количество циклов записи – 2. Цикл 1 – запись нулей. Цикл 2 - запись случайных кодов. Для классов защиты данных 4..6. Один цикл записи нулей.	
Алгоритм Брюса Шнейера (Bruce Schneier)	Количество циклов записи – 7. Цикл 1- запись единиц. Цикл 2 – запись нулей. Циклы 3..7 - запись случайных кодов.	
Алгоритм Питера Гутмана (Peter Gutman)	Количество циклов – 35. Циклы 1..4 - запись произвольного кода. Циклы 5..6 - запись кодов 55h, AAh. Циклы 7..9 – запись кодов 92h, 49h, 24h. Циклы 10..25 – последовательная запись кодов от 00, 11h, 22h и т.д. до FFh. Циклы 26..28 – аналогично циклам 7..9. Циклы 29..31 – запись кода 6Dh, B6h. Циклы 32..35 – аналогично циклам 1..4.	

Перезапись затрудняет процесс восстановления информации, но такая возможность остается.

Для восстановления информации требуется очень дорогое и сложное оборудование и ПО.

Коротко о физических основах восстановления информации

В современных НЖМД запись информации на магнитный диск производят **только** головки записи. При воздействии магнитного поля головки НЖМД происходит рост количества и размеров магнитных доменов, ориентированных по направлению этого поля. На магнитной поверхности под головкой создается информативная остаточная намагниченность, которая и регистрируется при считывании. Уровень поля головки меньше уровня насыщения магнитной среды, поэтому остаются магнитные домены сравнительно малого объема, ориентированные по направлению предшествующего магнитного воздействия. Магнитное поле этих доменов слабое и не влияет на результат считывания штатным контроллером. Однако эти домены могут быть обнаружены более чувствительными специальными головками (датчиками) или же выявлены при детальном анализе тонкой структуры магнитного поля, порождаемого участком рабочей поверхности накопителя.

На рис.1 показано рабочее место «реставратора» информации.

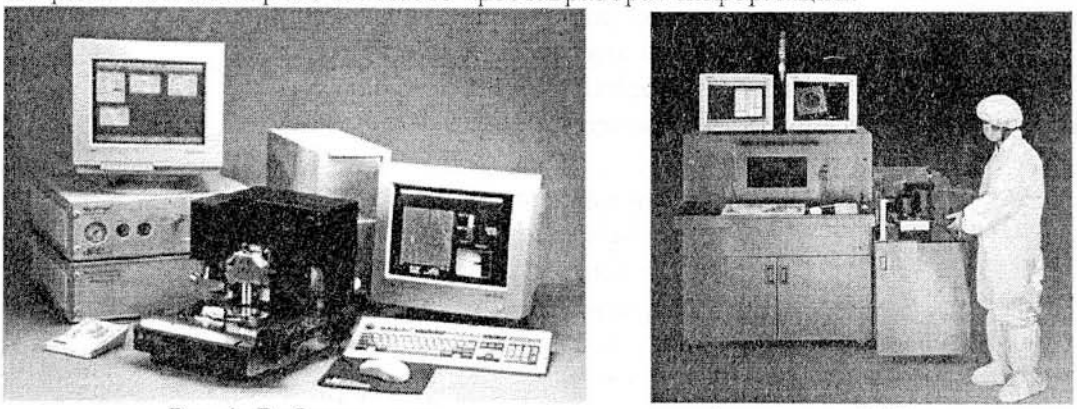

Рис.1. Рабочее место «реставратора» информации [12]

Перезапись информации на НЖМД может производиться как на ПК, так и вне его с помощью специальных приборов (например, EPOS Tester HDD – рис. 2.) [13]. В этом случае метод перезаписи можно назвать – программно-аппаратным.

Рис. 2. ЕПОС Тестер HDD с реализованным программно-аппаратным методом уничтожения информации перезаписью

Выводы по программным методам уничтожения информации на НЖМД [12].

Недостатки:

1) Низкая надежность уничтожения информации. После применения программных методов стирания информации перезаписью имеется возможность восстановления информации квалифицированным экспертом с помощью или без специальных средств.

2) Длительное время перезаписи информации носителя (десятки минут, часы). При многопроходной перезаписи время уничтожения информации для одного носителя умножается на количество проходов.

3) Перезапись информации возможна только на исправном НЖМД.

Достоинства:

1) Имеется возможность повторного использования НЖМД;
2) Низкая цена и стоимость эксплуатации ПО или специальных средств.

Принятие решения о выборе метода уничтожения информации часто связано с оценкой рисков. Поэтому выбор метода уничтожения информации путем перезаписи тесно связан с ответами на вопросы: «– Какова вероятность потенциальной угрозы? – Какие усилия может приложить злоумышленник для восстановления ограниченной к доступу информации? – Если его действия увенчаются успехом, каковы возможные последствия?»

Механические методы уничтожения информации на НЖМД

Часто, когда необходима повышенная надежность уничтожения информации, к НЖМД применяют механические методы уничтожения, при которых разрушается сам носитель информации.

Стоимость НЖМД значительно снизилась за последние годы. Поэтому, как и в случае гибких магнитных дисков, для многих компаний экономически может быть более целесообразно уничтожать их, а не удалять секретную информацию. Но здесь мы сталкиваемся с проблемой высокой стоимости оборудования для механического уничтожения и процессом контроля уничтожения в случае наличия этого оборудования в других компаниях.

Механические методы уничтожения информации подразделяются на:

- **Механического воздействия**. Измельчение носителя путем пропускания через устройство измельчения (шредер).

НЖМД разрушается механически так, чтобы исключить возможность прочтения информации каким-либо способом с его рабочих дисков.

При этом методе существует опасность, что при измельчении могут оставаться фрагменты, достаточно крупные, чтобы восстановить информацию в лабораторных условиях. Вскрытие корпуса гермокамеры в рабочем помещении (вне чистой комнаты) приводит к загрязнению пластин и выводу НЖМД через несколько часов из строя. В современном НЖМД диск стирается попавшей пылью до основы (прозрачной стеклянной подложки), как наждаком, при последующей работе после вскрытия гермокамеры (Рис. 3).

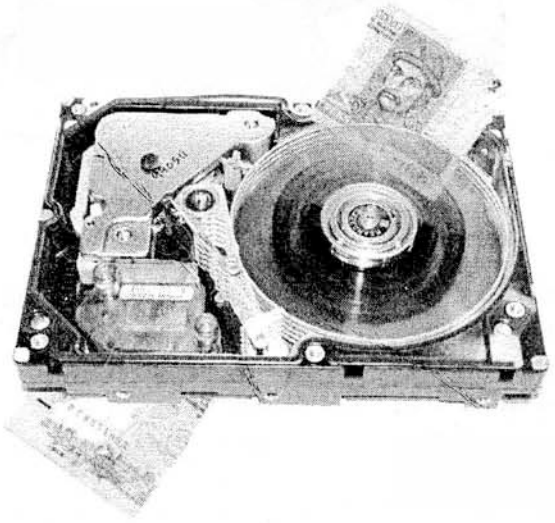

Рис. 3. Жесткий диск с разрушенным магнитным покрытием (стеклянная подложка)

Часто используемые на практике методы сверления отверстий и удары молотком по НЖМД, на самом деле не уничтожают вовсе или уничтожают малую часть информации.

- **Термический.** Нагревание носителя до температуры плавления в специальных печах.

При этом способе гарантия уничтожения информации наступает при разогреве носителя до температуры 800-1000°С. В этом случае информация становится абсолютно

невосстанавливаемой по целому комплексу причин, в том числе и из-за перехода магнитного материала покрытий через точку Кюри. Такой способ уничтожения информации может быть рекомендован для носителей, содержащих государственную тайну.

Пожар в помещении, где находятся ПК или костер из НЖМД не приводят к уничтожению информации Рис. 4 и 5.

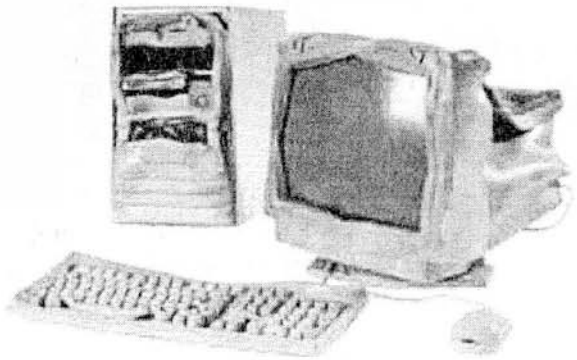

Рис.4. Полностью восстановленный и работоспособный компьютер после пожара в помещении. (Рекламная акция ООО ЕПОС, выставка EnterEx 2000)

Рис.5. Винчестеры компьютеров сгоревшего офиса. Информация была полностью восстановлена в сервис центре ООО ЕПОС (2001г.)

- **Пиротехнический.** Разрушение носителя взрывом.
- **Металлотермический.** Уничтожение основы носителя, на который непосредственно нанесено магнитное покрытые, высокой температурой самораспространяющегося высокотемпературного синтеза (СВС). При этом на основу наносится специальный слой термитного покрытия.
- Химический. Разрушение рабочего слоя или основы носителя химически агрессивными средами.
- Радиационный. Разрушение носителя ионизирующими излучениями.

В табл. 2 представлены основные показатели механических методов уничтожения информации на НЖМД.

Таблица 2

Методы уничтожения информации на НЖМД

Механический	Измельчение носителя, его разрушение механическим воздействием.	Разрушающий метод. Возможно гарантированное уничтожение.
Термический	Нагревание носителя до температуры разрушения его основы (или до точки Кюри)	Разрушающий метод. Гарантированное уничтожение.
Пиротехнический	Разрушение носителя взрывом	Разрушающий метод. Возможно гарантированное уничтожение. Проблема обеспечения безопасности оператора.
Металлотермический	Уничтожение основы носителя высокой температурой самораспространяющегося высокотемпературного синтеза (СВС).	Разрушающий метод. Гарантированное уничтожение.
Химический	Разрушение рабочего слоя или основы носителя химически агрессивными средами.	Разрушающий метод. Гарантированное уничтожение. Проблема обеспечения безопасности оператора.
Радиационный	Разрушение носителя ионизирующими излучениями	Разрушающий метод. Опасность облучения.

Одни из них экологически небезопасны, другие могут обеспечить высокую надежность уничтожения информации, но требуют настолько специфического и дорогостоящего оборудования, которое могут позволить себе лишь единичные корпоративные пользователи.

Во всех этих методах отсутствует возможность повторного использования НЖМД.

Физические методы уничтожения информации на НЖМД

В настоящее время оптимальным подходом для обеспечения надежности уничтожения информации без уничтожения носителя является использование физических средств, связанных с перестройкой структуры магнитного материала рабочих поверхностей носителя.

Для уничтожения информации на магнитных пластинах НЖМД необходимо устранить неоднородности вектора намагниченности участков рабочей поверхности, несущих информацию о предшествующих записях.

Указанное изменение структуры поля вектора намагниченности магнитного слоя может быть выполнено несколькими принципиально различными способами:

- путем быстрого нагрева материала рабочего слоя носителя до точки потери намагниченности носителя (точки Кюри);
- путем размагничивания рабочих поверхностей носителя;
- путем намагничивания рабочих поверхностей носителя до максимально возможных значений намагниченности (насыщения).
- комбинированный. Нагревание и намагничивание, либо нагревание и размагничивание.

Первый способ (нагревание) основывается на одном из важных эффектов магнетизма – при нагревании ферромагнетика до определенной температуры, превышающей точку Кюри, интенсивность теплового движения атомов становится достаточной для разрушения его самопроизвольной намагниченности, и он становится парамагнетиком. При этой температуре ферромагнитный материал рабочего слоя теряет свою остаточную намагниченность, и все следы ранее записанной информации гарантированно уничтожаются.

Температура, соответствующая точке Кюри большинства ферромагнитных материалов рабочего слоя носителей информации, составляет несколько сот градусов (Рис. 6).

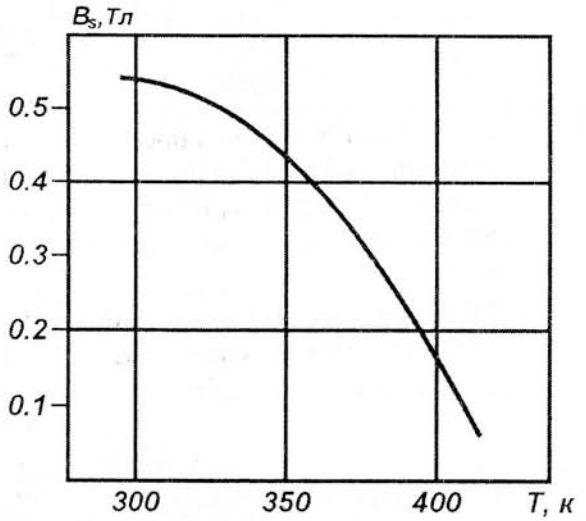

Рис. 6. Зависимость намагниченности магнитных покрытий от температуры

При этом надо учитывать, что каждый производитель НЖМД держит в секрете слои основы и состав ферромагнитного покрытия. Вероятнее всего, наиболее уязвимыми для температурных воздействий компонентами рабочего слоя и основы НЖМД окажутся связующие материалы органической природы. В этом случае при нагревании до высоких температур НЖМД выйдет из строя по причине плавления элементов конструкции, имеющих температуру плавления или деформации меньше точки Кюри для данного магнитного носителя.

Размагничивание рабочих поверхностей носителя

Размагнитить ферромагнетик можно и другим способом – поместить его в медленно убывающее переменное магнитное поле.

В случае с НЖМД возникают трудности, связанные с большой коэрцитивной силой (остаточной намагниченностью) ферромагнитного покрытия диска.

В источнике [14] производится расчет условий получения стационарных и убывающих магнитных полей, необходимых для размагничивания ферромагнитных материалов.

Мощность, потребляемая соленоидом, может быть найдена по формуле:

$$P = 10^{-6} H_m^2 a(\gamma_{Cu} / \gamma_o)$$

где a - радиус соленоида;

γ_o - удельная проводимость материала обмотки;

γ_{Cu} - удельная проводимость меди.

С помощью этого выражения легко подсчитать, что для получения стационарного магнитного поля с напряженностью $H_M = 4000 кА/м$ в соленоиде с радиусом 1 см с водяным охлаждением потребуется мощность 250 кВт.

Получение сильных стационарных полей в зазорах электромагнитов ограничено индукцией насыщения магнитопровода, составляющей около 2 Тл. В [14] приводится информация об электромагните разработки АН СССР, который создает поле напряженностью $1000 кА/м$ в рабочем объеме 18 $см^3$ и потребляет мощность из сети 36 кВт.

В случае использования мощного постоянного магнита на основе самарий-кобальт или сходных по характеристикам композиций на основе лантаноидов возникают технологические трудности. Расчеты показывают, что для создания равномерного поля в воздушном зазоре при размещении в нем НЖМД с максимальным формфактором до 87,5 мм (с учетом накопителей, используемых в серверах) необходим постоянный магнит сложной формы с концентратором поля. Учитывая технологические возможности современной промышленной базы, его создание принципиально возможно, но для единичного экземпляра или малой серии экономически нецелесообразно [1].

Более продуктивным является подход, связанный с намагничиванием рабочих поверхностей носителя до максимально возможных значений (насыщения) носителя.

Намагничивание. Способ основан на положении, что в случае НЖМД внешнее магнитное поле рассматривается как аналог поля, создаваемого магнитными головками при записи. Если характеристики внешнего поля будут превышать напряженность поля, создаваемого головками на такую величину, при которой произойдет магнитное насыщение материала поверхности диска, то все магнитные домены будут переориентированы по направлению этого внешнего поля и вся информация на НЖМД будет уничтожена.

Для ферромагнетиков характерен гистерезис при перемагничивании внешним магнитным полем. На Рис. 7 приведена основная характеристика ферромагнетиков – зависимость магнитной индукции B от напряженности H намагничивающего поля [15].

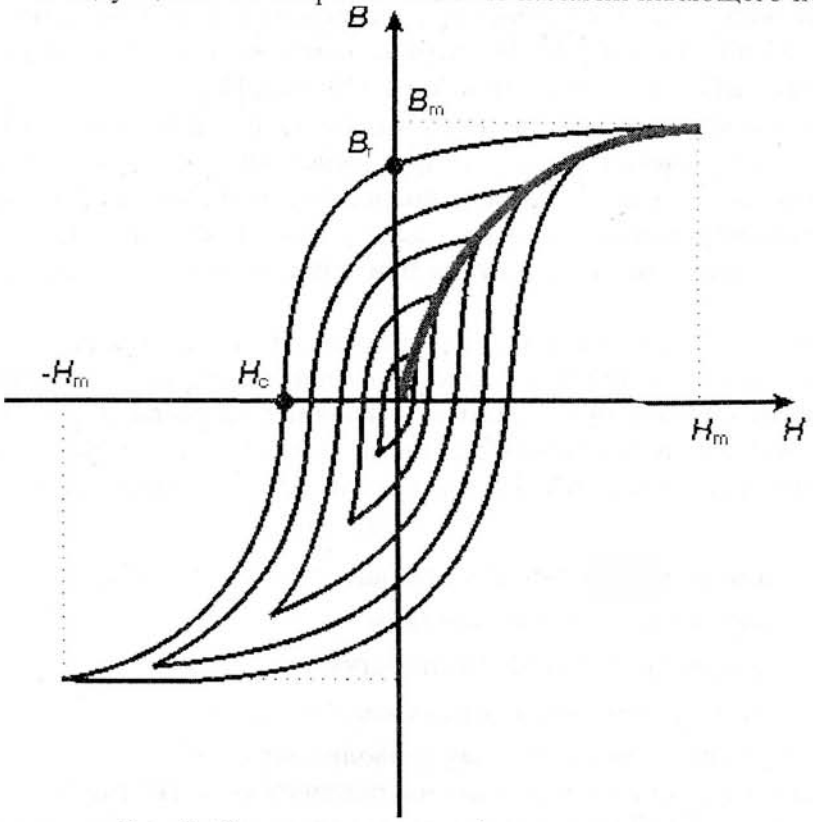

Рис. 7. Петля гистерезиса ферромагнетика

Под воздействием внешнего магнитного поля происходит ориентация элементарных магнитных полей, создаваемых круговым движением электронов в атомах

ферромагнетика. В результате увеличиваются размеры магнитных доменов, ориентированных по направлению внешнего поля. После прекращения внешнего воздействия изменения, произошедшие в размерах и ориентации магнитных доменов, частично сохраняются. Появляется остаточная намагниченность вещества – след, оставленный в ферромагнетике внешним воздействием. Именно эту остаточную намагниченность материала носителя регистрируют затем устройства, считывающие записанную информацию.

Зависимость намагниченности ферромагнетика от изменений внешнего магнитного поля носит нелинейный характер. Величина B_s характеризует величину индукции магнитного насыщения материала, при котором возрастание величины внешнего магнитного поля уже не приводит к изменениям в его доменной структуре, а значит к дальнейшему росту его намагниченности.

Величина B_r характеризует коэрцитивную силу – предельное остаточное магнитное поле (намагниченность) материала после прекращения воздействия на него внешнего поля, достаточного для насыщения ферромагнетика.

Физические основы процессов, происходящих в накопителе под влиянием внешнего магнитного поля, связаны с его конструктивными особенностями и спецификой применяемых материалов.

Ввиду того, что характеристика материала, из которого изготавливаются покрытия поверхностей современных НЖМД, как правило, фирмами-производителями не разглашаются, оценку величины напряженности намагничивающего поля приходится рассчитывать с некоторым запасом.

Расчет производится по аналогии с расчетом стирающего поля для магнитных лент [1]. Величина напряженности поля стирания для магнитной ленты при условии однопроходного воздействия превышает величину коэрцитивной силы в 4 раза.

Коэрцитивная сила современных ферромагнитных покрытий B_r – определена в диапазоне от 50 до 80 кА/м [16]. Поэтому величина поля намагничивания для НЖМД при однократном воздействии выбирается 200 – 320 кА/м [1].

При многократных воздействиях величина напряженности поля стирания может быть несколько меньше в силу действия накапливаемого уменьшаемого перемагничивания. На рис. 7, кроме основной петли гистерезиса, приведены и частичные циклы перемагничивания, которые дают нам представление, как многократным воздействием можно или размагнитить или намагнитить до насыщения ферромагнитное покрытие.

При расчете величины внешнего намагничивающего поля необходимо учитывать тот факт, что герметический металлический корпус (гермоблок) обычно изготавливаемый из алюминиевых сплавов будет оказывать влияние на внешнее магнитное поле. Расчеты показывают, что амплитуда напряженности поля H будет убывать при проникновении вглубь защитного корпуса НЖМД по экспоненциальному закону [17].

$$H_z = H_o e^{-kz},$$

где H_o - амплитуда напряженности магнитного поля, *А/м*;

z - расстояние от поверхности, м;

k $= \sqrt{\mu_o \mu_r \pi f \sigma}$ - коэффициент затухания;

f - частота электромагнитных колебаний, Гц;

σ - удельная электрическая проводимость, см/м.

Графики изменения амплитуды напряженности магнитного поля в зависимости от толщины корпуса НЖМД при различных длительностях воздействия приведены на рис. 8.

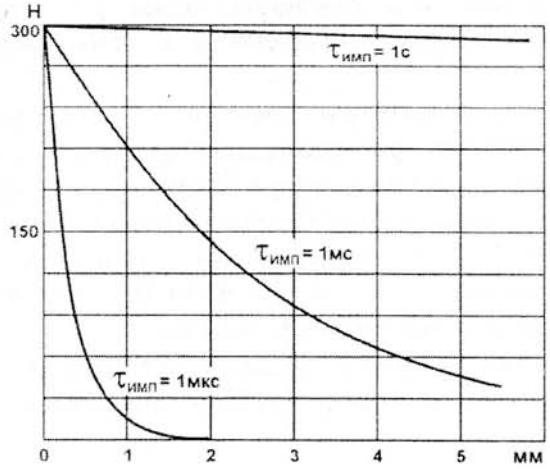

Рис. 8. Графики изменения амплитуды напряженности магнитного поля в зависимости от толщины корпуса НЖМД.

Следовательно, высокочастотные электромагнитные поля ($t_{имп} \leq 10 мкс$) распространяются фактически только в тонком поверхностном слое.

Постоянные и слабопеременные (с частотами менее 1 герца) магнитные поля проникают через защитный корпус без существенного ослабления. [1]

Импульсные намагничивающие установки [14] удовлетворяют вышеперечисленным требованиям. Они обеспечивают:

- Возможность создания сильных намагничивающих полей с малыми энергетическими затратами.
- Кратковременность воздействия импульсного поля на образец.
- Возможность помещения НЖМД целиком в камеру намагничивания;
- Возможность применения простых индукторных систем разомкнутого типа без магнитопровода;
- Формирования магнитного поля необходимой направленности.

Наиболее простыми импульсными источниками тока для намагничивающих устройств, являются источники, в которых энергия сети и емкостного накопителя поступает в виде импульса непосредственно в индуктор.

Блок-схема устройства намагничивания импульсного типа приведена на Рис. 9 [14].

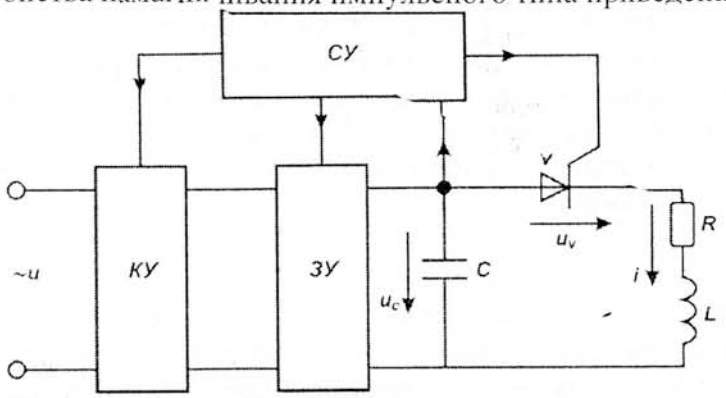

Рис. 9. Блок-схема устройства намагничивания импульсного типа

В такой установке емкостной накопитель, представляющий собой батарею конденсаторов с емкостью C, заряжается до необходимого напряжения от специального зарядного устройства (ЗУ).

Зарядное устройство подключается и отключается от сети с помощью коммутирующего устройства (КУ).

Процессы включения и отключения зарядного устройства от сети, управления емкостным накопителем энергии управляются и контролируются системой управления (СУ).

Разряд емкостного накопителя энергии C на индуктор с сопротивлением R и индуктивностью L производится после подачи отпирающего импульса на управляющий вентиль, работающей либо в ручном, либо в автоматическом режимах.

В этой схеме в качестве индуктора используется многовитковый соленоид. При расчете соленоида под R и L понимают суммарные эквивалентные параметры, учитывающие сопротивление и индуктивности подводящих проводов, вентиля, конденсаторов и контактных перемычек между ними.

Для полного уничтожения следов остаточной намагниченности носитель необходимо намагнитить до насыщения [18], а затем постепенно снизить напряженность поля до нуля.

В индукторе это будет происходить тогда, когда $R < 2\sqrt{L/C}$, т.е. индуктор будет работать в колебательном режиме переходного процесса.

Процесс разряда описывается формулами [14]:

$$\left.\begin{array}{l} u_C = u_V + Ri + Lpi; \\ i = -Cpu_C \text{ при } u_V \geq 0; \\ i = 0 \text{ при } u_V < 0. \end{array}\right\}$$

Задавая значения R, L, C получают необходимые параметры: амплитуду намагничивающего импульса I_m, длительность импульса t_0 и время нарастания тока t_m.

Несколько слов о направлении прилагаемого внешнего магнитного поля. Направление внешнего магнитного поля задается конструкцией и формой витков индуктора. Для наибольшей эффективности намагничивания внешнее поле должно прикладываться в той же плоскости, в которой работают головки записи НЖМД. В этом случае эффект намагничивания максимален.

Магнитное поле, генерируемое намагничивающими установками при достаточной амплитуде намагничивающего импульса приводит к уничтожению служебной разметки поверхности диска и данных в секторах. При этом НЖМД выходит из строя, так как механика привода не может функционировать без служебной разметки диска. Это обстоятельство приводит к невозможности проверки надежности уничтожения информации. Получить доступ к информации на пластинах жесткого диска можно только при помощи его головок в случае работоспособности привода и электроники НЖМД. Невозможность функционирования привода не обеспечивает гарантии подтверждения полного уничтожения информации. Убедиться в том, что информация уничтожена, позволяют только средства визуализации магнитных полей носителя. В [9, 11] эти вопросы рассматриваются подробно.

Выводы:

1) Размагничивание (намагничивание) – достаточно надежный метод уничтожения информации с поверхностей магнитных носителей при условиях:

- правильного применения размагничивателей (намагничивателей) с полями достаточной напряженности;

- обязательного применения средств визуализации магнитных полей носителядля контроля надежности уничтожения информации.

Список литературы

1. Беседин Д.И., Боборыкин С.Н., Рыжиков С.С. Предотвращение утечки информации, хранящейся в накопителях на жестких магнитных дисках. Специальная техника. №1/2001.

2. Причины потери информации с электронных накопителей. С. Коженевский

3. www.seagate.com

4. www.fujitsu.com

5. www.maxtor.com

6. www.wdc.com

7. Блиц-опрос. Сколько ПК продано в Украине в 2002 году. Компьютерное обозрение. Издательский дом ITC. С. 48, 58.

8. Anthony Thornton. End-of-Life Data Security in the Enterprise. Data Security Whitepaper. http://www.redemtech.com/

9. Методы сканирующей зондовой микроскопии для исследования поверхностей носителей информации. С.Коженевский. Реєстрація, зберігання і обробка даних. 2002, Т.4, №3, стр.23-40.

10. Экспертное заключение по итогам анализа устройства быстрого уничтожения информации на магнитных носителях «Стек». Испытательная лаборатория в системе сертификации ФСБ России.

11. Методы визуализации магнитных полей носителей информации. С.Коженевский. Реєстрація, зберігання і обробка даних. 2002, Т.4, №4, стр. 48-60.

12. Monteith G. Heaton, F. Michael Serry. Scanning Probe/Atomic Force Microscopy: Technology Overview and Update. Digital Instruments, Veeco Metrology Group. http://www.di.com

13. www.epos.kiev.ua

14. Нестерин В.А. Оборудование для импульсного намагничивания и контроля постоянных магнитов. – М.: Энергоатомиздат, 1986, с. 88

15. Болдырев А.И., Сталенков С.Е. Надежное стирание информации – миф или реальность? Защита информации. Конфидент. №/2001. С. 38.

16. Котов Е.П., Руденко М.И. Носители магнитной записи. Справочник. М.: Радио и связь, 1990г.

17. Абакумов А.А. Магнитная интроскопия М.: Энергоатомиздат., 1996г.

18. Seamus Ross, Ann Gow. Digital Archaeology: Rescuing Neglected and Damaged Data Resources. A JISC/NPO Study within the Electronic Libraries (eLib) Programme on the Preservation of Electronic Materials. February 1999. University of Glasgow. http://www.hatii.arts.gla.ac.uk/

19. Болдырев А.И., Василевский И.В., Сталенков С.Е. Методические рекомендации по поиску и нейтрализации средств негласного съема информации. М.:ЗАО НПЦ Фирма «НЕЛК». 2001.

20. Рохманюк В.М., Фокин Е.М. Чисто? Чисто и быстро! Защита информации. Конфидент, 1998 №5

21. Рохманюк В.М., Фокин Е.М. Аппаратура экстренного уничтожения записей на магнитных носителях. БДИ, 2000 №5

22. Рохманюк В.М., Фокин Е.М. Способ стирания записей на магнитном носителе и устройство для его осуществления. Патент на изобретение RU № 2144223

23. Рохманюк В.М., Фокин Е.М. Устройство для стирания записи на магнитном носителе. Свидетельство на полезную модель №18796.

24. Справочник по электротехническим материалам / Под ред. Ю.В. Корицкого, В.В. Пасынкова, Б.М. Тареева. Т.3. Л.: Энергоатомиздат. ЛО, 1988. С.10.

25. Физическая энциклопедия. Т.1. М.: Советская энциклопедия. 1990.
26. Физическая энциклопедия. Т.2. М.: Советская энциклопедия. 1990.
27. Физическая энциклопедия. Т.3. М.: Советская энциклопедия. 1992.
28. Физическая энциклопедия. Т.4. М.: Советская энциклопедия. 1994.
29. Кнопфель Г. Сверхсильные импульсные магнитные поля. Перевод с английского Николаева Ф.А., Свириденко Ю.П. М.: Мир. 1972.

Поступила 29.01.2003г.

УДК 621.397.27

Попов С. А.

СИСТЕМА ЦВЕТНОГО ТЕЛЕВИДЕНИЯ С ВРЕМЕННЫМ УПЛОТНЕНИЕМ КОМПОНЕНТНЫХ СИГНАЛОВ ИЗОБРАЖЕНИЯ КОСМИЧЕСКИХ СТАНЦИЙ «МИР», «АЛЬФА» .

Введение

С начала полетов пилотируемых космических кораблей одной из основных проблем явилась необходимость обмена борт-земля, земля-борт визуальной информацией. Так уже при полете Ю.А.Гагарина использовалась телевизионная система с разрешением 100 строк. В дальнейшем на пилотируемых космических кораблях (ПКК) использовались стандартные системы черно-белого телевидения. Для передачи изображения на землю применялась система ретрансляции через наземные приемные станции (НИП) и спутники-ретрансляторы «Молния». При подготовке совместного советско-американского полета по программе «Союз»-«Аполлон» во Всесоюзном НИИ телевидения была разработана последовательная по полям система передачи цветного изображения, основанная на использовании черно-белой телекамеры с вращающимся светофильтром. Однако, ее значительным недостатком явилось цветовое расслоение изображения при передаче подвижных изображений. Попытка применить цветные телекамеры, работающие в стандартных системах СЕКАМ, ПАЛ оказалась неудачной, так как выяснилось, что система ретрансляции НИП'ы-«Молнии» в ряде случаев не обеспечивает нужной для этих систем полосы пропускания. Особо остро проблема встала при подготовке полета японского журналиста в 1990 г., где одним из условий контракта было обеспечение передачи качественного цветного изображения. Поскольку изменение качественных параметров инфраструктуры ретрансляции влекло неоправданно высокие экономические затраты, специалистами Ракетно-Космической Корпорации «Энергия» было принято решение о необходимости применения специальной системы цветного телевидения, позволяющей найти компромисс между качеством цветного изображения и возможностями существующей системы ретрансляции. После анализа ряда предложенных систем к концу 1989 г. была выбрана система с временным уплотнением сигналов яркости и цветности, предложенная автором настоящей статьи [1,2]. Успешная реализация этой системы (шифр «Кулик») дала толчок к дальнейшему развитию бортовых систем цветного