УДК 621.96

БЕЗОПАСНОСТЬ ХРАНЕНИЯ ИНФОРМАЦИИ НА ЖЕСТКИХ ДИСКАХ

Сергей Коженевский
ООО ЕПОС

Аннотация: **Описаны методы восстановления доступа к информации на жестких дисках, подробно рассмотрены вопросы гарантированного уничтожения данных и предотвращения несанкционированно доступа к информации, хранящейся на жестких дисках. Рассмотрены перспективные способы восстановления информации, приведены практические рекомендации по организации процедуры уничтожения информации.**
Summary: **This paper describes the methods for renewal of data accessibility on hard disk drives, in detail covers the issues on secure data erasure and prevention of unauthorized access to information stored on hard drives. Also are considered the prospective means for data recovery and the practical recommendations on data erasure routine organization are given.**
Ключевые слова: **Информация, информационная безопасность, жесткий диск, информационные сейфы**

I Проблемы и технологии восстановления доступа к информации, хранимой на НЖМД

Технологический процесс восстановления доступа к информации всегда начинается с **диагностики технического состояния накопителя**, включающей в себя: диагностику рабочих поверхностей, тестирование контроллера, выполнения тестов чтения данных. После определения причины утраты доступа к данным выбирается соответствующий способ его восстановления.

Если по результатам диагностики техническое состояние жесткого диска соответствует нормам (накопитель исправен), а потеря информации произошла вследствие программного сбоя (воздействие вирусов, неквалифицированные действия пользователей, сбои операционной системы), то для восстановления доступа к информации используется специализированное программное обеспечение, позволяющее получить доступ к данным на диске на уровне команд интерфейса. В этом случае говорят о восстановлении доступа к данным на логическом уровне.

При наличии достаточного опыта во многих случаях восстановить доступ к информации на исправном жестком диске можно и без применения специальных утилит, пользуясь только DiskEdit. Справедливости ради необходимо заметить, что опыт необходим и при применении специальных утилит. В автоматическом режиме даже широко известная утилита «Tiramisu» не в состоянии правильно восстановить последовательность кластеров, содержащих тот или иной файл. Тем не менее, в случае полной исправности жесткого диска доступ к данным можно восстановить и самостоятельно. Важно только понимать, что с первой попытки угадать правильную последовательность кластеров не удается. Поэтому, чтобы не потерять информацию окончательно, все работы по восстановлению информации можно проводить только с копией жесткого диска.

Именно поэтому следующим шагом после диагностики накопителя является **создание точной копии (образа) жесткого диска**. Создание копии жесткого диска необходимо не только с целью обезопасить свою работу. Поверхность диска может иметь отдельные повреждения. Эти повреждения опасны тем, что сопровождаются появлением внутри герметической камеры жесткого диска мельчайших твердых частиц. Эти частицы приводят к новым повреждениям поверхности, причем этот процесс носит лавинообразный характер. В результате после нескольких часов работы накопителя на значительной площади поверхности дисков рабочий слой стирается полностью (рис. 1).

Технология восстановления доступа к информации с неисправного жесткого диска существенно отличается от восстановления данных на логическом уровне. Во многих случаях восстановить работоспособность накопителя удается лишь на непродолжительное время. Например, в результате «шлепка» головки повреждается как сама головка, так и поверхность диска. Чаще всего именно это и является причиной рассмотренной выше неисправности. Выбитые из поверхности диска осколки, находясь внутри герметичной камеры, продолжают разрушать рабочий слой, что очень быстро приводит к полному отказу накопителя [1].

Если при первых признаках неисправности жесткий диск приносят в сервисный центр, то, как правило, удается спасти большую часть информации. Более того, удается восстановить некоторую часть информации

даже с поврежденных участков пластин жесткого диска. Для этого при создании копии жесткого диска используется технология адаптивного копирования.

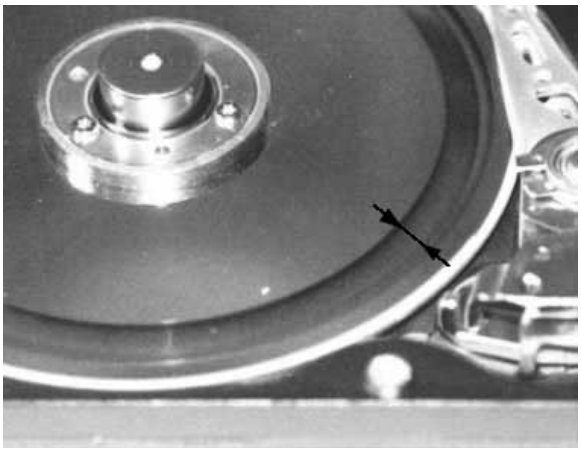


Рисунок 1 – Стертый рабочий слой в зоне 3000 – 10000 дорожек

Суть ее заключается в быстром копировании информации с неповрежденных участков и последующим многократном (до 100 раз) считывании информации с поврежденных участков. Затем проводится статистическая обработка результатов считывания сбойных секторов с помощью метода максимального правдоподобия. Критерием успешного восстановления информации является достижение заданного порогового значения коэффициента правдоподобия. В некоторых случаях после процедуры адаптивного копирования требуется проведение работ по восстановлению данных на логическом уровне.

Повреждение поверхности пластин жесткого диска является, наверное, самой распространенной и опасной неисправностью, но далеко не единственной. Жесткие диски могут выходить из строя по множеству причин. Это и нарушение теплового режима, и повышенная влажность, и производственные дефекты, и «шлепки» головки из-за внешних ударных воздействий, и износ вследствие интенсивной работы. Более подробно ознакомиться с устройством и причинами выхода из строя жестких дисков можно в [2].

В табл. 1 приведены некоторые типичные неисправности жестких дисков и способы восстановления доступа к информации.

Таким образом, все случаи восстановления доступа к информации на отказавших жестких дисках можно разделить на две большие группы: требующие вскрытия герметичной камеры и не требующие ее вскрытия.

В случае, когда вскрытие герметичной камеры не требуется, проблема восстановления информации решается заменой контроллера или чипа управления двигателем на аналогичный. В принципе, такую операцию квалифицированный пользователь может выполнить самостоятельно. Необходимо найти полный аналог неисправного жесткого диска и аккуратно переставить с него контроллер.

Восстановление информации с повреждениями в камере (обрыв или повреждение головок, отказ коммутатора, дефекты и износ рабочей поверхности) требует вскрытия гермоблока, что, в свою очередь, требует применения специального оборудования и, в первую очередь, наличия «чистой комнаты» - помещения, в котором строго контролируется концентрация взвешенных в воздухе мельчайших пылинок.

В чистой комнате выполняются работы по восстановлению информации, связанные со вскрытием камер накопителей на жестких дисках:

- замена головок или блока головок;
- замена микросхемы предусилителя-коммутатора;
- адаптивное копирование информации;
- замена головок и блока головок.

В нерабочем состоянии головки прижимаются к пластинам в специальной зоне, называемой зоной парковки. Выход головок в зону парковки выполняется автоматически при снижении скорости вращения двигателя ниже номинальной или пропадании напряжения питания. Поскольку поверхности дисков и головки изготавливаются очень гладкими (шероховатость порядка 5Å), то иногда наблюдается эффект «прилипания» головки к диску. В этом случае, при подаче напряжения на накопитель головки не успевают оторваться от поверхности начинающих вращение дисков и происходит их перекос или обрыв. Повреждения головок могут возникать и в результате «шлепка» головки, вызванного внешним ударным воздействием на

рабочий жесткий диск. В обоих случаях головка начинает царапать поверхность диска, повреждая его поверхность (рис. 2).

Таблица 1 – Типовые неисправности жестких дисков и способы восстановления доступа к информации

Неисправности	Основные признаки	Особенности восстановления
Частичное повреждение головок (без обрыва)	Накопитель не инициализируется или инициализируется неустойчиво, при этом периодически теряет готовность, а данные не читаются или читаются неустойчиво.	Замена блока головок на аналогичный. Требуется вскрытие камеры
Обрыв головок	Накопитель не инициализируется. Возможно прослушивание посторонних звуков при раскрутке шпиндельного двигателя.	Замена блока головок на аналогичный. Требуется вскрытие камеры
Выход из строя интегральной микросхемы усилителя коммутатора.	Накопитель не инициализируется. Шпиндельный двигатель раскручивается нормально.	Замена ИМС усилителя коммутатора. Замена блока головок на аналогичный. Требуется вскрытие камеры
Повреждение рабочих поверхностей	Накопитель не инициализируется или инициализируется неустойчиво. Данные читаются неустойчиво. Шпиндельный двигатель раскручивается нормально.	Адаптивное копирование информации. Требуется вскрытие камеры
Выход из строя ИМС управления шпиндельным двигателем.	Шпиндельный двигатель не раскручивается	Замена ИМС управления шпиндельным двигателем. Без вскрытия камеры
Выход из строя ИМС поддержки внешнего интерфейса.	Накопитель не инициализируется, или инициализируется, но не выдает признака готовности к работе и не выполняет команды.	Замена ИМС поддержки внешнего интерфейса. Без вскрытия камеры
Выход из строя ПЗУ контроллера	Накопитель не инициализируется. Шпиндельный двигатель не раскручивается.	Замена ПЗУ контроллера с записью кода точного аналога. Без вскрытия камеры
Полный выход из строя контроллера накопителя.	Накопитель не инициализируется, шпиндельный двигатель не раскручивается.	Замена контроллера целиком на точный аналог. Без вскрытия камеры

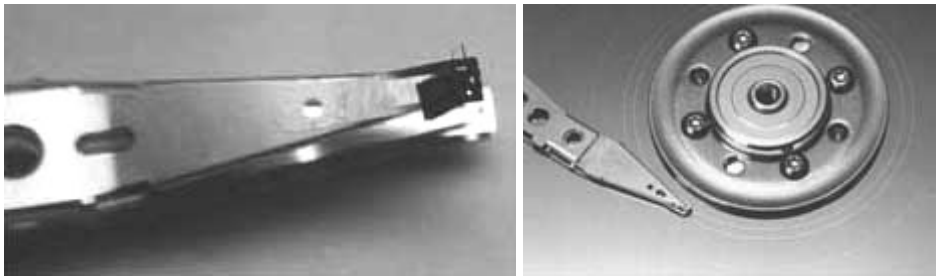


Рисунок 2 – Перекос головки и вызываемые им повреждения поверхности диска

Чтобы восстановить информацию с такого накопителя, необходимо заменить поврежденную головку или блок головок полностью. В более старых моделях жестких дисков каждая головка в блоке при производстве юстировались под свою рабочую поверхность, поэтому даже в одном блоке головки могли быть позиционированы по-разному. При замене блока головок было необходимо калибровать все четыре головки, что отнимало много времени, при этом при попытках прочитать данные еще больше повреждалась поверхность диска. Чтобы решить эту проблему, было разработано прецизионное устройство для замены и юстировки отдельных головок (рис. 3). Это устройство позволяет удалить поврежденную головку, запрессовать на ее место рабочую и откалибровать ее с точностью до единиц микрон.

В современных жестких дисках с высокой плотностью записи такой точности юстировки головки уже недостаточно, поскольку ширина дорожек записи составляет порядка десятых долей микрон. Кроме того, благодаря достижениям в технологиях производства жестких дисков блоки головок в накопителях одной серии практически идентичны. Поэтому при повреждениях отдельных головок полностью заменяется весь блок головок.

Рисунок 3 – Прецизионное устройство для замены головок и работы по замене головок в чистой комнате

Замена микросхемы предварительного усилителя-коммутатора

Распространенной причиной отказов жестких дисков является выход из строя предварительного усилителя-коммутатора в результате бросков напряжения или неправильного подключения напряжения питания. В старых моделях накопителей микросхема коммутатора находилась внутри камеры возле разъема для подключения к контроллеру. Это позволяло выполнять ее замену без снятия блока головок.

Чтобы обеспечить минимальное затухание сигнала считывания, в современных жестких дисках усилитель-коммутатор размещают непосредственно на блоке головок (рис. 4). В этом случае перед заменой микросхемы необходимо снять весь блок головок, чтобы избежать перегрева дисков при пайке и потери информации. Некоторые производители используют бескорпусные микросхемы коммутаторов, которые не подлежат замене – в этом случае заменяют весь блок головок.

а) б)

Рисунок 4 – Варианты исполнения блоков головок: а) с корпусным усилителем-коммутатором; б) с бескорпусным усилителем-коммутатором

Адаптивное копирование информации

Замена любого элемента жесткого диска негативно сказывается на его характеристиках. Из-за невозможности точно откалибровать блок головок увеличивается количество ошибок чтения. После замены усилителя-коммутатора обычно снижается отношение сигнал/шум, что тоже приводит к росту ошибок. Поэтому при копировании данных с отремонтированного жесткого диска на технологический целесообразно применять алгоритм адаптивного копирования. Но даже при применении алгоритма адаптивного копирования головка часто «зацикливается» на некоторых дорожках, многократно пытаясь прочитать один и тот же сектор. Это приводит к тому, что на считывание информации с такого жесткого диска уходит очень

много времени – в среднем сутки, а иногда и до месяца непрерывной работы. Если выполнять такое копирование в обычном помещении, головка достаточно быстро сотрет рабочий слой до основы.

Герметизация камер некоторых жестких дисков обеспечивается с помощью специальной липкой ленты, наклеиваемой по периметру корпуса накопителя. При повреждении этой ленты (при неосторожном обращении при транспортировке или установке в узкие карманы некоторых корпусов компьютера) возможна непреднамеренная разгерметизация камеры (рис. 5).

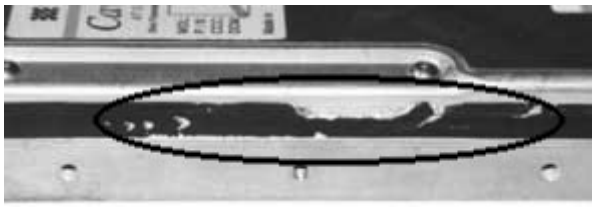


Рисунок 5 – Повреждения герметизирующей ленты, приводящие к разгерметизации камеры жесткого диска

Нарушение герметизации может приводить к попаданию внутрь камеры пыли, разрушающей головки и рабочие поверхности дисков. Такой накопитель может еще работать некоторое время, однако обычно очень скоро начинается лавинообразный процесс возникновения сбойных секторов и он выходит из строя. Тем не менее, если своевременно обратиться в центр восстановления информации, информацию еще можно будет спасти. Жесткий диск вскроют в чистой комнате, аккуратно вычистят попавшую внутрь камеры пыль. Затем данные будут переписаны на технологический жесткий диск.

Следует отметить, что любое вскрытие камеры жесткого диска, даже без замены его узлов, приводит к ухудшению его работы и впоследствии к выходу его из строя [1, 3]. Средний срок службы накопителя, камера которого вскрывалась, не превышает двух-трех месяцев. Затем начинается быстрый рост количества сбойных секторов, увеличивается вероятность ошибок чтения и жесткий диск выходит из строя окончательно. Именно поэтому вскрытие камеры жесткого диска и ремонт элементов, расположенных в камере, производится только с целью восстановления информации, а не с целью восстановления его работоспособности.

В последнее время участились случаи, когда пользователи пытаются самостоятельно восстановить информацию или отремонтировать жесткий диск, вскрывая при этом его камеру. Это **всегда** приводит к окончательному нарушению его работоспособности и очень затрудняет восстановление данных. Например, отпечатки пальцев с зеркальной поверхности пластины удалить уже практически невозможно (рис. 6). Из этого рисунка видно, что информацию в начале диска, где обычно хранится операционная система, еще можно восстановить, а пользовательские данные в середине и конце диска могут быть утеряны безвозвратно.

Рисунок 6 – Отпечатки пальцев на рабочей поверхности жесткого диска

Подавать напряжение питания на накопитель с открытой камерой вне чистой комнаты недопустимо. Воздушный поток захватывает частицы пыли, которые начинают разрушать рабочий слой. В зависимости от скорости вращения дисков частицы пыли уничтожат рабочий слой за один-два часа, стирая его до основы, из которой изготовлены диски (рис. 7). Информацию в этом случае восстановить невозможно.

Вскрытие камеры жесткого диска можно производить только в чистой комнате, где строго

контролируется количество частиц, взвешенных в воздухе.

Описанные выше методы позволяют в большинстве случаев восстановить информацию. Однако, возможности всех этих методов ограничиваются точностью механического позиционирования головок чтения. В настоящее время разработаны и более мощные способы восстановления информации, основанные на визуализации магнитных полей рассеяния. Эти способы позволяют создавать визуальное представление рабочих поверхностей носителя с высоким разрешением, достаточным для побитового исследования информации [4]. Известно более десятка таких методов, но при высоких плотностях записи данных современных жестких дисков наибольшими возможностями по восстановлению информации обладает метод снятия магнитной сигналограммы, основанный на магнитной силовой микроскопии. Наибольшую трудность при применении магнитной силовой микроскопии вызывает необходимость совмещения множества изображений различных участков поверхности диска. В настоящее время для ускорения этого процесса выпускаются магнитные силовые микроскопы со специально разработанными механизмами поворота поверхности жесткого диска относительно рабочей зоны микроскопа (рис. 8).

Рисунок 7 – Рабочий слой жесткого диска полностью уничтожен. Материал пластины – стекло

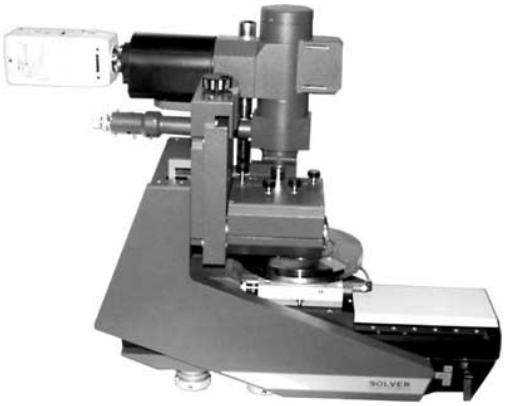


Рисунок 8 – Магнитный силовой микроскоп для визуализации рабочих поверхностей жестких дисков

С помощью подобных систем возможно восстановление информации в ряде случаев даже после того, как на место хранения восстанавливаемого файла многократно записаны новые данные.

Несколько менее мощным, но зато значительно более дешевым является метод Биттера (метод «магнитных чернил»). Разрешающая способность при визуализации магнитных полей методом Биттера ограничивается размерами ферромагнитных частиц в суспензии, используемой в процессе визуализации. Тем не менее, применяемая в центре восстановления информации компании ЕПОС суспензия позволяет осуществлять визуализацию магнитных полей для жестких дисков объемом до 4ГБ. Более того, для дисков большей емкости можно получить изображение с детализацией, достаточной для анализа общей структуры диска и состояния его рабочей поверхности. В частности, на рис. 9 приведена фотография магнитной сигналограммы поверхности жесткого диска объемом 2 ГБ.

На изображении хорошо видны дорожки с записанной информацией. Более того, на краях дорожки видны остатки предыдущих записей на данный участок поверхности диска. Поэтому возможно частичное восстановление информации, даже при записи «поверху» восстанавливаемой информации нового файла.

II Уничтожение информации, хранимой на НЖМД

В настоящее время на развитие индустрии защиты информации (ЗИ) тратятся миллионы долларов. 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.

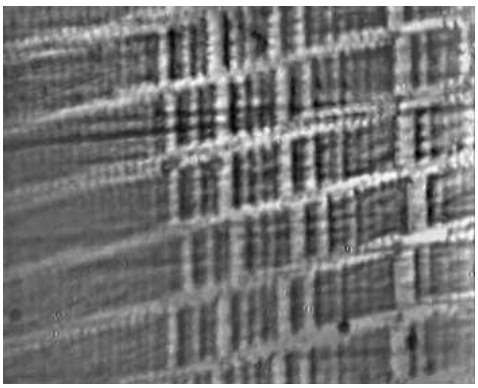


Рисунок 9 – Участок поверхности жесткого диска с информационными дорожками

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. 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 непосредственно связаны с технологиями обработки, передачи и утилизации информации, хранящейся на НЖМД [5].

Утечка информации при замене исправного 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 операционной системы старый ПК можно будет использовать на новом месте как автоматизированную систему начального уровня. Однако 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 ПК не находит применения в организации, он может быть продан полностью или по частям учреждениям, которые могут использовать его целиком или отдельные комплектующие (сервисные центры, начинающие пользователи и т. д.).
3. Дарение ПК. Очень часто устаревшие ПК безвозмездно передаются детским учреждениям или благотворительным организациям.

Во всех этих случаях старые компьютеры (вместе с жесткими дисками) вывозятся вместе со всеми данными, на защиту которых были потрачены деньги и время; в крупных организациях это происходит почти каждый день.

В то время, как существуют не только законы, но и аппаратные средства, запрещающие или

препятствующие несанкционированному доступу к 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 компьютеров не знают, что простое удаление файлов или даже переформатирование жесткого диска 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 открытия доступа 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 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 компьютера 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 [6]). 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.

Большинство дисков ломаются в гарантийный период и должны быть заменены по гарантии при условии сохранности пломб и отсутствия 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 к ней нежелателен. Даже если представить, что в гарантийный период выйдет из строя 10% НЖМД при количестве проданных в Украине в 2002г. – 500 000 шт., 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 НЖМД, 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 ЗИ. 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 [7], существуют основные положения и условия защиты информации:

1. необходимость физической защиты НЖМД;
2. систематический контроль и ведение отчетности.

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.

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;
- дату и время уничтожения;
- ФИО исполнителя;
- использованную методику уничтожения.

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

1. физическая защита информации, включающая в себя инвентаризацию и ограничение 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 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, [4]).

Способы уничтожения информации на НЖМД делятся на три большие группы:

1) **программные**, в основу которых положено уничтожение информации, записанной на магнитном носителе, посредством штатных средств записи информации на магнитных носителях;

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.

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.

По способу воздействия на НЖМД способы уничтожения информации делятся на:

1. без разрушения конструктива и поверхностей НЖМД;
2. с разрушением НЖМД.

Программные способы уничтожения информации на НЖМД

1) Уровень 0 (начальный уровень). Наиболее простая и часто применяемая форма уничтожения информации на НЖМД. Вместо полного стирания НЖМД в загрузочный сектор, в 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 для анализа 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 эффект краев дорожек.

Восстановить информацию, удаленную этим методом, стандартными средствами невозможно. Для восстановления требуются специальные знания и оборудование [4, 8].

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. 2.

Таблица 2 – Сравнительная таблица алгоритмов уничтожения данных

Алгоритм	Содержание алгоритма	Примечания
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 инвертированного кода. Цикл 3 – запись случайных кодов.	NISPOM запрещает использование этого алгоритма для уничтожения данных с грифом:"СОВ.СЕКРЕТНО" Альтернативные способы (в соответствии с NISPO): - размагничивание; - физическое разрушение
Стандарт VISR, 1999 г. (Гемания)	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)	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.

Перезапись информации на НЖМД может производиться как на ПК, так и вне его с помощью специальных приборов (например, EPOS Tester HDD – рис. 10). В этом случае метод перезаписи можно назвать программно-аппаратным.

Выводы по программным методам уничтожения информации на НЖМД:

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.

Рисунок 10 – ЕПОС Тестер HDD с реализованным программно-аппаратным методом уничтожения информации перезаписью

Достоинства.

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

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 методы механического воздействия, термического, пиротехнического, металлотермического.:

Методы 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.

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

Методы термического воздействия. Нагревание носителя до температуры плавления в специальных печах.

При этом способе гарантия уничтожения информации наступает при разогреве носителя до температуры 800-1000ºС. 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. 11, 12).

- **Методы пиротехнического воздействия.** Разрушение носителя взрывом.
- **Методы металлотермического воздействия.** Уничтожение основы носителя, на который непосредственно нанесено магнитное покрытие, 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.

Рисунок 11 – Компьютер после пожара в помещении. Полностью восстановлен в ООО ЕПОС

Рисунок 12 – Винчестеры компьютеров сгоревшего офиса. Информация была полностью восстановлена в сервисном центре ООО ЕПОС (2001 г.)

В табл. 3 представлены основные показатели механических методов уничтожения информации на НЖМД.

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

При использовании всех этих методов отсутствует возможность повторного использования НЖМД.

Физические способы связаны с физическими принципами цифровой записи на магнитный носитель, и основаны на перестройке структуры магнитного материала рабочих поверхностей носителя. Наиболее широко применяется воздействие на рабочую поверхность жесткого диска магнитным полем. В силу определенных особенностей конструкции жестких дисков и применяемого в них способа записи в настоящее время применяется в основном воздействие мощным магнитным импульсом с целью намагничивания рабочей поверхности до насыщения.

Таким образом, в зависимости от того, от каких угроз необходима защита, можно выбрать соответствующий уровню угрозы метод уничтожения информации. При этом достоверность уничтожения информации должна быть подтверждена тем или иным способом. Особенно это относится к методам уничтожения информации, при которых внешне диск остается неповрежденным. Наибольшую трудность вызывает подтверждение надежности уничтожения информации путем воздействия магнитного импульса. Фактически в этом случае пригодны только различные методы визуализации магнитных полей рассеяния. При этом, в отличие от рассмотренных выше задач восстановления информации, разрешающая способность метода визуализации может быть и не очень высокой. Ведь для подтверждения гарантии уничтожения информации ее не обязательно полностью восстанавливать. Но если в процессе контроля качества уничтожения будут обнаружены остатки информации, то при применении более сложных методов ее можно будет восстановить. Поэтому для задач контроля качества уничтожения информации наиболее пригоден метод Биттера. Более того, задачу контроля качества уничтожения информации (по крайней мере, при уничтожении информации воздействием магнитного импульса) можно еще более упростить. Действительно, синхродорожка на поверхности жесткого диска записывается при изготовлении диска гораздо более мощным

полем, чем записываются данные во время эксплуатации диска. Поэтому, если на поверхности диска не обнаружены остатки синхродорожки, то можно гарантировать, что все данные тем более уничтожены. Наличие же синхродорожки после визуализации магнитных полей методом Биттера может быть обнаружено даже без применения микроскопа (рис. 13).

Таблица 3 – Механические 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

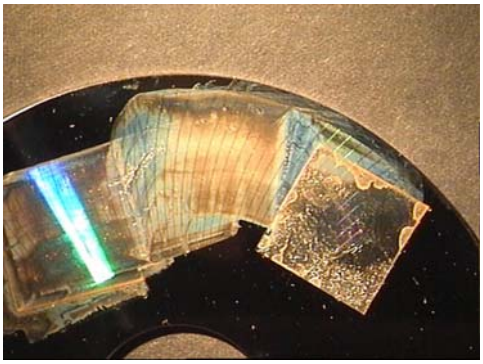


Рисунок 13 – Визуализация магнитных полей рабочей поверхности жесткого диска. Этим методом, в частности, ЕПОС проверял качество уничтожения информации при отработке параметров станции комплексного технического обслуживания жестких дисков

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?»

III Обеспечение невозможности доступа к информации, хранимой на НЖМД

Наряду с проблемами восстановления и уничтожения информации на жестких дисках существует и проблема обеспечения невозможности несанкционированного доступа к информации, хранящейся на жестких дисках. Существует несколько путей решения этой проблемы, требующих применения различных организационных и технических мер.

Наилучший и самый простой способ – это не оставлять диски с критичной информацией без контроля.

Для реализации такого способа существуют специальные фреймы для быстрой установки и снятия жестких дисков. Такие фреймы могут устанавливаться в корпус компьютера и подключаться к компьютеру интерфейс USB или FireWare (рис. 14).

а) **б)**

Рисунок 14 – Варианты исполнения съемных жестких дисков:
а) внутренний фрейм; б) внешний жесткий диск с подключением через интерфейсу USB 2.0

Жесткий диск в съемном фрейме хранится в охраняемом помещении (в секретном отделе) и выдается пользователю под расписку только на время работы.

Современные жесткие диски весьма критичны к любым ударам и тряскам. Поэтому регулярные перемещения жесткого диска приводят к значительному снижению его срока службы. Однако, этот недостаток не настолько принципиален, как некоторые думают. По крайней мере, при выходе диска из строя информацию можно восстановить. Главное, информация всегда остается под контролем: всегда известно кто и в какое время работал с данным диском. Более того, очень легко решаются проблемы, связанные с увольнением сотрудников и с необходимостью доступа к критичной информации нескольких сотрудников.

Второй способ обеспечения невозможности несанкционированного доступа к информации – это ее шифрование. Шифрование может осуществляться аппаратно, средствами BIOS компьютера (например, в ноутбуках Fujitsu-Siemens), средствами операционной системы (Windows 2000, Windows XP) или специализированными программами (PGP, WinRar 2.6). С точки зрения надежности ограничения несанкционированного доступа принципиальной разницы в выборе способа шифрования нет. Главный недостаток ограничения доступа к информации путем шифрования – это то, что на самом деле проблема ограничения несанкционированного доступа к информации не решается, а заменяется на сходную проблему – обеспечения невозможности несанкционированного доступа к ключам шифрования. Частично проблемы, связанные с ограничением доступа к ключам шифрования решаются путем хранения ключей на внешних носителях. Ввиду чрезвычайно низкой надежности хранения информации ключи нежелательно хранить на дискетах (хотя и до сих пор ключи довольно часто хранятся именно на дискетах). Для хранения ключей шифрования сейчас разработано множество малогабаритных и весьма надежных носителей. В частности, могут применяться неспециализированные устройства (Flash-карты) или специально разработанные носители: TouchMemory, SmartCard, ключи HASP, e-Token (рис. 15).

Сохранность носителей ключевой информации может быть обеспечена организационными мерами (хранение носителей с ключевой информацией в секретном отделе).

В ряде случаев в качестве носителей ключевой информации (или как дополнительная мера защиты ключей) применяются биометрические датчики. В частности, для транспортировки информации с ограниченным доступом выпускаются жесткие диски в защищенном от вибраций и ударов исполнении, информация на которых хранится в зашифрованном виде, а в качестве ключа шифрования используется отпечаток пальца владельца информации (рис. 16).

Шифрование позволяет надежно решить задачу ограничения доступа к информации (при правильной организации генерации, хранения и распределения ключей). Однако при этом возникают специфические проблемы.

Любой носитель информации, в том числе и применяемый для хранения ключей, имеет конечное значение надежности. При утрате же ключей шифрования (в том числе и при выходе из строя носителя)

зашифрованная информация теряется безвозвратно. По крайней мере, ее восстановление в большинстве случаев становится экономически нецелесообразным.

а) **б)**

в)

Рисунок 15 – Виды носителей ключевой информации: а) HASP; б) TouchMemory; в) e-Token

Рисунок 16 – Накопитель LoqDrive 250 SPR со встроенным сканером отпечатка пальца

Существует и другая проблема. При выходе из строя накопителя, при нарушении логической структуры диска восстановить зашифрованную информацию гораздо сложнее, чем открытую. По сути, задача восстановления данных на исправном накопителе сводится, в основном, к задаче определения правильного порядка чередования кластеров жесткого диска, содержащих восстанавливаемый файл. Поэтому для восстановления зашифрованной информации помимо обычно применяемых для восстановления устройств и программного обеспечения необходимо иметь действующий комплект системы шифрования и правильные ключи шифрования. В случае же неисправности накопителя некоторую часть информации восстановить иногда невозможно. Многие алгоритмы шифрования работают по принципу «сцепления блоков», когда для дешифрования определенного блока данных необходимо знать предыдущий блок данных. Поэтому при восстановлении данных с неисправного накопителя возможны ситуации, когда вследствие потери незначительной части зашифрованной информации невозможно восстановить и остальную ее часть.

На практике может встретиться и весьма специфическая задача предотвращения доступа к данным в экстремальной ситуации. Например, во время ведения боевых действий может возникнуть угроза захвата техники противником. В этом случае все данные и ключевая информация должны быть немедленно уничтожены. Время для подготовки к уничтожению и уничтожения данных, как правило, оказывается ограниченным. Уничтожение жестких дисков путем взрыва или сжигания не всегда приводит к

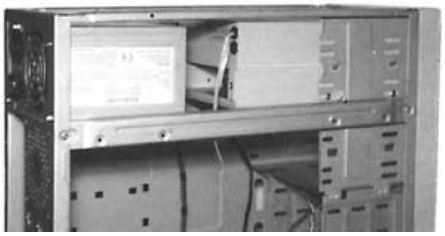
невозможности восстановления информации. Поэтому самым действенным способом уничтожения информации в экстремальных условиях является быстрое стирание информации путем воздействия на носитель мощного магнитного импульса.

Чтобы сократить время от момента возникновения угрозы до момента уничтожения информации многие фирмы выпускают специализированные «информационные сейфы», специальные камеры для установки жесткого диска, оборудованные устройством быстрого стирания информации магнитным импульсом. Камера может устанавливаться в компьютер или выполняться во внешнем исполнении (рис. 17 а, б). В любом случае установленный в «информационном сейфе» диск подключается к компьютеру, и в нормальных условиях обеспечивается нормальная работа с жестким диском. В случае же возникновения экстремальной ситуации достаточно нажатия одной кнопки для полного гарантированного уничтожения информации.

Такой метод уничтожения реализован, в частности, в станции комплексного технического обслуживания СКТО жестких дисков, выпускаемой ООО ЕПОС (рис. 17 в). Готовится к серийному выпуску также вариант СКТО НЖМД с возможностью подключения жестких дисков к компьютеру для реализации функций «информационного сейфа». Варианты исполнения «информационных сейфов» приведены на рис. 17.

При эксплуатации подобных устройств необходимо помнить, что при правильном изготовлении «информационного сейфа» магнитным импульсом не только гарантированно уничтожается вся информация, хранящаяся на жестком диске, но и сам жесткий диск приводится в непригодное для дальнейшей эксплуатации состояние. Более того, как и любая техника, «информационный сейф» может отказать. В этом случае он может как не выполнить свои функции в экстремальной ситуации, так и самопроизвольно запустить функцию уничтожения информации, когда это не требуется. Информация может быть также уничтожена и по ошибке оператора (нечаянное нажатие кнопки уничтожения). В любом случае восстановление информации и дальнейшая эксплуатация жесткого диска становятся невозможными. Поэтому пользоваться данными устройствами необходимо осторожно, и только в тех случаях, когда угрозу захвата диска с информацией невозможно блокировать другим способом.

а)



б)

в)

Рисунок 17 – Варианты исполнения «информационных сейфов»:
а) внешнее исполнение на 5 жестких дисков; б) внутреннее исполнение; в) СКТО НЖМД

Литература ***1.*** *Подводные камни DIY recovery. С. Чеховский. Информационная безопасность офиса, Научно практический сборник, вып. 1 «Технические средства защиты информации», К.: ООО «ТИД «ДС», 2003.* ***2.*** *Винчестер под микроскопом. Ю. Мул, В. Поречный. Информационная безопасность офиса, Научно-*

практический сборник, вып. 1 «Технические средства защиты информации», К.: ООО «ТИД «ДС», 2003. ***3.*** *High Precision Cleaning for the Disk Drive Industry. Bill Lambert. Whitepaper, Kerry Ultrasonics Ltd, 2000.* ***4.*** *Методы сканирующей зондовой микроскопии для исследования поверхностей накопителей информации и восстановления данных. С. Коженевский, С. Прокопенко. Информационная безопасность офиса, Научно-практический сборник, вып. 1 «Технические средства защиты информации», К.: ООО «ТИД «ДС», 2003.* ***5.*** *Беседин Д. И., Боборыкин С. Н., Рыжиков С. С. Предотвращение утечки информации, хранящейся в накопителях на жестких магнитных дисках. Специальная техника. №1/2001.* ***6.*** *Жесткий диск – прямой канал утраты информации. С. Коженевский. Информационная безопасность офиса, Научно практический сборник, вып. 1 «Технические средства защиты информации», К.: ООО «ТИД «ДС», 2003.* ***7.*** *Anthony Thornton. End-of-Life Data Security in the Enterprise. Data Security Whitepaper. http://www.redemtech.com/* ***8.*** *Методы визуализации магнитных полей носителей информации. С. Коженевский. Реєстрація, зберігання і обробка даних. 2002, Т. 4, № 4, стр. 48-60.*

УДК 654.1 (045)

ЦЕНТР ОБСЛУГОВУВАННЯ ТЕЛЕФОННИХ ВИКЛИКІВ ЯК ЕКОНОМІЧНО ЕФЕКТИВНА ПЛАТФОРМА ДЛЯ КЕРУВАННЯ КОМПЛЕКСНОЮ СИСТЕМОЮ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Георгій Конахович, Володимир Чуприн
Національний авіаційний університет

Анотація: **Обґрунтовано доцільність використання центрів обслуговування телефонних викликів (Call Centers) як платформ для створення централізованих систем керування територіально розподіленими інформаційними системами.**
Summary: **The expediency of use of the centres of service of telephone calls (Call Centers) as platforms for creation централизованних of control systems is territorial by the allocated information systems.**
Ключові слова: **Інформація, система керування, інформаційна безпека.**

I Вступ

Проектування та створення засобів централізованого керування підсистемами технічного захисту інформації (ТЗІ) (що мають назву відповідно до моделі мережного керування ISO - Security Management) в сучасних складних територіально розподілених інформаційних системах (ІС), наприклад в корпоративних телефонних мережах, побудованих на основі телефонних мереж загального користування (PSTN), як правило, здійснюється в комплексі із засобами керування іншими чотирма підсистемами підтримки функцій експлуатації цих ІС (тобто, у комплексі з Fault, Configuration, Performance and Accounting Management) [1]. Ці засоби у переважній більшості випадків мають унікальну і громіздку логічну структуру, а вартість їхньої реалізації настільки велика, що є “непід’ємною” навіть для найбільших організацій України. Проблема керування розподіленими ІС утруднюється ще й тим, що реально на практиці для побудови мереж керування цими ІС використовуються лише мережі пакетної комутації із застосуванням популярного SNMP-протоколу прикладного рівня, або, в останній час, із застосуванням WEB-технологій (у гетерогенних розподілених середовищах іноді також використовується технологія керування CORBA і ін.) [2]. Звісно, що інформація користувача в загальнодоступних каналах мереж пакетної комутації у порівнянні з каналами мереж комутації каналів є більш уразливою з точки зору ТЗІ, тому що абонентські канали, які утворюються за допомогою засобів мереж пакетної комутації, є логічно (а не фізично) відокремленими і тому доступними для неавторизованих суб’єктів з невеликими ресурсними можливостями. З урахуванням вищезазначеного є доцільним здійснити спроби створення систем керування на основі використання мереж із комутацією каналів, які є менш уразливими з боку неавторизованих користувачів.

II Постановка завдання

Хоча засоби керування, що реалізують універсальну концепцію TMN, підтримувану MCE-T у рамках семирівневої моделі взаємодії відкритих систем [3], могли б знайти застосування в мережах комутації каналів, але внаслідок їхньої особливої складності (і, отже, високої вартості) вони в експлуатаційній практиці, як правило, не використовуються. Найбільш поширені заходи щодо протидії загрозам в мережах з пакетною комутацією – це використання технологій закриття каналів, базованих на криптографічних