ИНФОРМАТИКА

УДК 537.611

ОБЗОР СУЩЕСТВУЮЩИХ ПРОГРАММНЫХ МЕТОДОВ УНИЧТОЖЕНИЯ ИНФОРМАЦИИ НА МАГНИТНЫХ НОСИТЕЛЯХ

В.А. КОНДРАТЁНОК, О.В. ЧУРКО

Военная академия Республики Беларусь

Поступила в редакцию 6 февраля 2008

Отражено современное состояние проблемы уничтожения программными методами цифровой информации, хранящейся на магнитных носителях. Приведена систематизация программных методов уничтожения информации. Кратко рассмотрены основные особенности методов и их отличия.

Ключевые слова: безопасность информации, уничтожение информации программными методами, магнитный носитель информации.

Введение

Магнитные носители информации (МНИ) — магнитные ленты, жесткие и гибкие магнитные диски — по-прежнему остаются наиболее распространенным типом носителей информации. Интерес к ним во многом определяется тем, что, несмотря на наличие альтернативных носителей (оптические диски, флэш-память и др.), они обладают относительной дешевизной, надежностью и быстротой доступа к хранящейся информации, а, следовательно, будут применяться еще достаточно долго.

Однако увеличение объемов хранящейся на МНИ и обрабатываемой информации создает предпосылки для несанкционированного доступа к ней, в том числе в ходе ремонта, гарантийного обслуживания и после выведения их из эксплуатации и списания.

В связи с этим представляется необходимым проведение обзора и систематизации существующих методов уничтожения информации, хранящейся на магнитных носителях. При этом авторы считают целесообразным в настоящей статье остановиться на программных методах уничтожения информации, так как они считаются наиболее распространенными.

Методы уничтожения информации на МНИ

Методы уничтожения информации, хранящейся на МНИ, делятся на механические, физические и программные [1].

Механические методы связаны механическим повреждением физического носителя информации, подложки. К ним относят:

– механическое воздействие (прессование, эрозирование поверхности и др.);

– термический метод (переплавка или обжиг дисков);

– пиротехнический метод;

– химический метод (химическое травление);

– радиационный метод.

При использовании перечисленных методов отсутствует возможность повторного использования МНИ и в большинстве случаев обеспечивается гарантированное уничтожение ин-

формации. Необходимо отметить также отсутствие неоднозначностей при оценке этой гарантированности, так как информация уничтожается вместе со своим носителем.

Физические методы связаны с физическими принципами цифровой записи на МНИ и основаны на перестройке структуры магнитной рабочей поверхности носителя. Наиболее широко применяется воздействие на рабочую поверхность МНИ магнитным полем (постоянным или переменным). В связи с определенными особенностями конструкции жестких дисков и используемого в них способа записи в настоящее время обычно применяется воздействие мощным магнитным импульсом с целью намагничивания рабочей поверхности до состояния насыщения [1, 2]. Уничтожение информации происходит за счет намагничивания носителя импульсным кратковременно создаваемым мощным электромагнитным полем определенной величины и ориентации.

К преимуществам физических методов уничтожения информации — надежность, простота, а также гарантированность уничтожения информации на любых магнитных носителях, в том числе и на работающих в момент уничтожения [1].

Программные методы уничтожения информации на МНИ используются в тех случаях, когда необходимо обеспечить возможность дальнейшего использования МНИ после уничтожения хранящейся на них информации, так как обычно, о чем свидетельствуют результаты проведенного анализа литературы, программные методы, при всех их достоинствах, не обеспечивают гарантированность уничтожения информации.

Обобщенный анализ программных методов уничтожения информации

В основу программных методов уничтожения информации положено уничтожение информации, записанной на магнитном носителе, посредством штатных средств записи информации. При этом МНИ после уничтожения информации может быть повторно использован в "штатном" режиме. Уничтожение информации производится ее перезаписью. Перезапись — это процесс записи несекретных данных в область памяти, где ранее содержалась конфиденциальная информация [1].

Можно выделить три уровня (степени) уничтожения информации программными методами.

Начальный уровень уничтожения информации (уровень 1).

В большинстве случаев (в зависимости от настройки параметров операционной системы) "обычный" пользователь применяет двухшаговую процедуру удаления информации: на первом шаге стираемый файл перемещается в корзину (*Recycle Bin*), откуда в дальнейшем он может быть восстановлен самим пользователем средствами операционной системы; на втором шаге пользователь "очищает" корзину, опасно заблуждаясь, что после этого восстановление удаленной информации невозможно. Однако при этом удаленный файл не уничтожается физически. Операционная система просто помечает область диска, занятую данным файлом, как свободную и доступную для записи очередного файла. Хранимая в файле информация при этом не стирается.

Уровень 1 — это наиболее простая и часто применяемая форма уничтожения информации на магнитных носителях. Вместо полной очистки жесткого диска в загрузочный сектор, основную и резервную таблицы разделов записывается последовательность нулей.

В этом случае данные на диске не уничтожаются, хотя доступ к ним осложняется. Полный доступ к информации на магнитных носителях может быть восстановлен с помощью специального программного обеспечения, производящего анализ секторов диска (*Norton DiskEdit, Disk Investigator, WinHex, Recovery Expert, Restoration и* т.д.).

Промежуточный уровень уничтожения информации (уровень 2).

Выполнением данной процедуры при помощи, к примеру, программы *Restoration*,ограничивают мероприятия по уничтожению информации так называемые "продвинутые" пользователи. В ходе ее производится запись последовательности нулей или единиц в секторы данных. При этом уничтожается не только загрузочная область, но и данные.

При этом уничтоженную информацию восстановить без применения специальных средств практически невозможно. Однако упомянутые специальные технические средства су-

ществуют. Это может быть метод магнитной силовой микроскопии [3], метод магнитооптической визуализации на основе феррит-гранатовых пленок и т.д.

В основе возможности восстановления информации, уничтоженной перезаписью, лежат:

– ошибки оператора и неправильное использование программного обеспечения (ПО);

– отказ ПО перезаписывать все адресуемое пространство МНИ;

– наличие остаточной информации в дефектных секторах (зоны остаточной информации могут возникать, к примеру, на краях дорожки, как показано на рис. 1 и 2 [3]. Визуализировав такие зоны, можно при использовании специального оборудования восстановить удаленную информацию);

– возможность анализа зон остаточной намагниченности и исследования эффекта краев дорожек (в структуру многих форматов записи заложено существование междорожечных защитных промежутков, предотвращающих наложение и взаимное влияние дорожек. Информация считывается только с информационных дорожек, а сигнал от междорожечных промежутков рассматривается как шум. Пример такой несанкционированной междорожечной записи приведен на рис. 3 [3]).

Заключительный уровень уничтожения информации (уровень 3).

Процедура осуществления заключительного (третьего) уровня уничтожения информации программными методами заключается в использовании нескольких (в зависимости от применяемого алгоритма) циклов перезаписи информации и применяется, в основном, "корпоративными" пользователями, имеющими необходимость хранить и обрабатывать, в том числе, и конфиденциальную информацию.

Последовательности, прописываемые в секторы данных, стандартизированы. Наиболее часто употребляемые сведены в таблицу [1]. Чем больше циклов перезаписи информации применяется, тем сложнее восстановить удаленные данные. Это связано с неточностью позиционирования головки, так как чем больше раз головка перезапишет данные, тем выше вероятность того, что она сотрет зоны остаточной намагниченности на краях дорожки (рис. 1, 2).

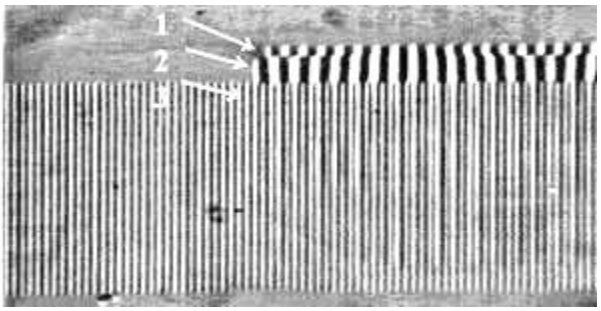

Рис. 1. Результаты визуализации зон остаточной информации: *1, 2* — остатки предыдущих записей; *3* – новая запись

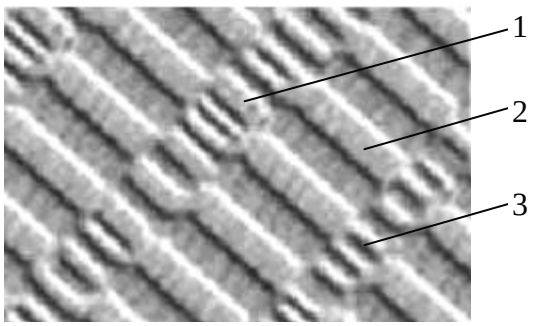

Рис. 2. Результаты визуализации магнитного рельефа поверхности жесткого диска при помощи метода магнитной силовой микроскопии: *1, 3* — остатки предыдущих записей; *2* — новая запись

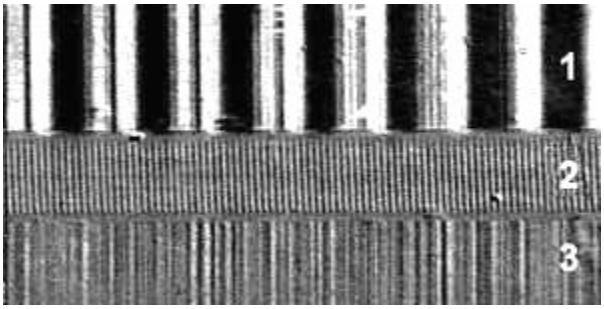

Рис. 3. Несанкционированная запись в междорожечном промежутке: *1, 3* — информационные дорожки; *2* — запись в междорожечном промежутке

Стоит, однако, отметить, что хотя многократная перезапись информации на магнитных носителях и значительно затрудняет процесс восстановления информации, но такая возможность остается.

Алгоритмы уничтожения данных

Алгоритм	Содержание алгоритма
NISPOM (руководство по защите информации министерства обороны США 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
VISR (стандарт 1999 г., Германия)	Количество циклов записи — 3 цикл 1 — запись нулей; цикл 2 — запись единиц; цикл 3 — запись кода с чередованием нулей и единиц
ГОСТ Р50739-95 (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	Количество циклов записи — 7 цикл 1 — запись единиц; цикл 2 — запись нулей; циклы 3–7 — запись случайных кодов
Алгоритм Питера Гутманна	Количество циклов — 35 циклы 1–4 — запись произвольного кода; циклы 5–6 — 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.

Заключение

Анализ представленного материала позволяет определить основные достоинства и недостатки программных методов уничтожения информации.

К достоинствам программных методов уничтожения информации относят:

– возможность повторного использования магнитного носителя;

– низкую цену ПО или специальных средств и стоимость их эксплуатации.

Недостатки программных методов следующие:

– низкая надежность уничтожения информации (после применения перезаписи имеется возможность восстановления информации квалифицированным экспертом с помощью или без специальных средств. Это связано с тем, что на участках рабочей поверхности носителя остаются микрообласти, ориентированные по направлению предшествующего внешнего магнитного воздействия. Остаточное намагничивание этих областей сравнительно невелико и не может регистрироваться штатным устройством. Однако при детальном анализе тонкой структуры магнитного поля, создаваемого исследуемым участком рабочей поверхности носителя, следы предшествующих внешних магнитных воздействий обнаруживаться могут. Эти следы и позволяют при необходимости восстановить уничтоженную процедурой любого уровня информацию);

– большое время перезаписи информации носителя (при многопроходной перезаписи информации время уничтожения для одного носителя в количество раз, равное числу проходов и может составлять несколько часов);

– возможность перезаписи информации только на исправном магнитном носителе.

В связи с этим пользователям рекомендуется тщательно оценивать возможный риск утечки конфиденциальной информации и ущерб от него при планировании мероприятий по уничтожению информации в ходе эксплуатации МНИ, их ремонта, гарантийного обслуживания, утилизации МНИ и т.д.

THE PROGRAM METHODS OF DESTROY OF INFORMATION ON MAGNETIC CARRIES REVIEW

V.A. KONDRATYONOK, O.V. CHURCO

Abstract

The modern conditions of a problem of destroy of information on magnetic carries is reflected. The systematization of program methods of destroy of information is reduced. The basic features of methods and their difference are briefly considered.

Литература

1. Информационная безопасность офиса: Науч.-практ. сб. Вып. 1. Технические средства защиты информации. Киев, 2003.
2. *Тикадзуми С.* Физика ферромагнетизма. Магнитные характеристики и практические применения / Пер. с японского. М., 1987.
3. *Коженевский С.Р., Прокопенко С.Д.* Методы сканирующей зондовой микроскопии для исследования поверхностей накопителей информации и восстановления данных. Электронный ресурс. Режим доступа: http://epos.kiev.ua/pubs.