УДК 621.391

Защита результатов физических экспериментов от несанкционированного копирования при хранении информации на гибких магнитных дисках

А. И. Астайкин, А. В. Круглов, А. П. Мартынов, В. Б. Профе
Российский федеральный ядерный центр — ВНИИ экспериментальной физики, Саров, Россия

Предложен метод кодирования информации по ГОСТ 28147—87 в режимах гаммирования с обратной связью и выработки имитовставки вместе с классическим изменением структуры дискеты.

Проблема обеспечения защиты результатов физических экспериментов от несанкционированного копирования при хранении информации на гибких магнитных дисках требует принятия соответствующих решений. В настоящей статье для решения этой проблемы предлагается использовать симбиоз из классического изменения структуры дискеты (привязка к временным параметрам чтения/записи, нестандартной разметки дорожек, изменение межсекторной дистанции) и кодирования информации по ГОСТ 28147—89 в режиме гаммирования с обратной связью и выработки имитовставки. При таком методе кодирования изменение одного бита во входном потоке инормации приводит к изменению всего выходного потока, так как кодирование n-го блока информации зависит от кодированного $(n-1)$-го блока.

Чтобы более ясно понять суть метода защиты информации на гибких магнитных дисках от копирования, рассмотрим отличия в стандартной структуре дискеты и структуре, реализованной в данном методе.

На стандартной дискете после форматирования можно выделить четыре основные области, а именно:

загрузочный сектор (boot area);
область таблицы размещения файлов (FAT area);
корневой каталог (directory area);
область данных (data area).

Загрузочный сектор всегда является первым сектором на дискете. Именно сюда записывается информация о том, как организована дискета. За счет этого операционная система позволяет работать с большим набором гибких дисков, организованных по-разному.

Назначения некоторых байтов загрузочного сектора, которые описывают организацию дискеты, приведены ниже:

11—12 байт — число байт в секторе;
13 байт — число секторов в кластере;
14—15 байт — число резервных секторов;
16 байт — число копий FAT;
17—18 байт — число позиций в корневом каталоге;
19—20 байт — число секторов на диске;
21 байт — код типа диска.

Следующая важная область FAT — таблица размещения файлов, в которой операционная система назначает секторы для размещения различных файлов. В этой таблице для каждого сектора имеется своя запись, которая содержит информацию о том, занят сектор файлом или нет, если да, то каким именно,

а также указывается информация о плохих секторах. Размер таблицы зависит от размера диска. Чем выше емкость диска, тем больший размер должен быть у таблицы размещения файлов для хранения информации обо всех секторах диска. Для надежности таблиц размещения файлов может быть несколько. Обычно для стандартной дискеты емкостью 1,44 Мб (3,5″) таких таблиц две.

В корневом каталоге хранится информация о файлах, каталогах, времени и дате их создания, размеры и другие необходимые сведения.

Каждой позиции каталога отводится 32 байта. Назначение каждого байта приведено ниже:

1—8 байт — имя файла;
9—11 байт — расширение имени;
12 байт — атрибуты файла;
13—22 байт — в резерве операционной системы;
23—24 байт — время создания;
25—26 байт — дата создания;
27—28 байт — начальный кластер;
29—32 байт — размер файла.

Все остальное дисковое пространство, не занятое служебными областями (*B*oot *A*rea, FAT *A*rea, *D*irectory *A*rea), является областью данных, в которых хранится информация.

При использовании метода по защите информации на гибких магнитных дисках от копирования создается структура дискеты, которая отличается от стандартной. При форматировании дискеты создаются следующие разделы: системная область и область данных.

В системной области указывается размер файла в байтах, его имя и расширение, пароль, с которым данный файл был зашифрован, информация о порядке расположения секторов и плохих секторах.

Системная область и область с данными хранятся в зашифрованном виде.

Применение классического метода изменения параметров дисковода пресекает возможность просмотра дискеты обычными средствами, которые работают со стандартными форматами дискет. Поэтому такую дискету нельзя скопировать, не применяя специальных программ.

Так, например, применяя программу DISK EXPLORER, можно проанализировать логическую структуру дискеты и прочитав каждый сектор, сделать отдельные копии секторов, находящихся на дискете, в файлы. Но получение полного объема информации, записанной на дискете, не представляется возможным, поскольку последовательность расположения секторов с данными пользователю не известна, в отличие от стандартных дискет, где при записи файлов ДОС формирует таблицу размещения файлов, в которой указывается последовательность расположения секторов для каждого файла. Это создаст большое множество комбинаций при переборе всех секторов. К тому же каждый сектор кодирован в режиме гаммирования с обратной связью и его декодирование будет зависеть от декодирования предыдущего сектора, последовательность расположения которых не известна. Таким образом, чтобы получить доступ к файлу, необходимо переставить в нужном порядке сектора и расшифровать их.

Чтобы изменить режим работы дисковода, необходимо модифицировать содержимое определенных ячеек оперативной памяти.

По адресу 0000h:0078h: находится адрес, указывающий на таблицу данных, которые используются контроллером дисковода при работе с дискетой. При изменении этих параметров можно работать с нестандартными форматами дискет.

В данном методе используется форматирование с параметрами, отличающимися для каждого сектора.

Два сектора используются для хранения системной информации (размер, полное имя файла, информация о порядке следования секторов и плохих секторах, пароль, с которым был зашифрован файл).

Во время форматирования проверяется качество записи и считывания сектора, так как на дискете могут быть поврежденные сектора и, следовательно, изменится допустимый объем на дискете. После этого вычисляется объем свободного места на диске и сверяется с размером записываемого файла.

При восстановлении файла запрашивается пароль у пользователя. С введенным им паролем декодируется системная область и проверяется пароль, введенный и полученный при декодировании. При несовпадении работа завершается. Иначе выставляются параметры для дисковода, и происходит декодирование файла, записанного на диск.

Основным преимуществом разработанного метода является высокая криптографическая стойкость данных, записываемых на диск. Такая стойкость достигнута благодаря применению алгоритму криптографического преобразования по ГОСТ 28147—89. Применяя дополнительный режим выработки имитоприставки согласно алгоритму криптографического преобразования по ГОСТ 28147—89, можно защитить данные, находящиеся на диске, от имитации.

На основе описанного метода было разработано и отлажено необходимое программное обеспечение, реализующее на практике работу данного метода. В программное обеспечение входят программы записи информации на диск и чтения информации с диска. В данных программах, кроме введения режимов шифрования информации, время чтения и записи уменьшено на 10 % по сравнению со стандартными программами, работающими с гибкими магнитными дисками.

Используемая литература

1. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования ГОСТ 28147—89. Государственный комитет СССР по стандартам. М., 1989.

2. *Конхейм А. Г.* Основы криптографии. — М.: Радио и связь, 1989.

3. Организация и современные методы защиты информации/Под общей редакцией С. А. Диева, А. Г. Шавлова. Концерн "Банковский деловой центр". М., 1998.

Protection of results of physical experiments against the non-authorized copying at a storage of the information on floppy disks

A. I. Astaikin, A. V. Kruglov, A. P. Martynov, V. B. Profe
RFNC — Resesrch Institute of Experimental Physics, Sharov, Russia

The method of information coding on GOST 28147—87 in gamma-correction modes with a feedback and simulated embedding together with classical change of diskette structure is offered.