Література: ***1.*** *Мартыненко С. В., Шелест М. Е. Классификация стеганометодов визуальной среды//Науково-технічний журнал "Захист інформації". – 2001. - № 4. – С. 4-11.* ***2.*** *Хорошко В. О., Азаров О. Д., Шелест М. Е., Яремчук Ю. Є. Основи комп'ютерної стеганографії. – Вінниця: ВДТУ, 2003. 143 с.* ***3.*** *Брауде-Золотарем Ю. М. Исследование возможностей сокращения объема телевизионного сигнала за счет использования свойств зрения: Автореф. дис. канд. тех. наук. – М., 1960. – 15 с.* ***4.*** *Майданюк В. П. Разработка алгоритмов и аппаратных средств систем сжатия телевизионных изображений: Автореф. канд. тех. наук. – Винница, 1993. – 22 с.* ***5.*** *Майданюк В. П. и др. Кодирование изображений в компьютерных системах обработки информации. – К., 1996. – 16 с. – Деп. В Укр ІНТЕІ 16.11.98, № 144 – Уі96.* ***6.*** *Прэтт У. Цифровая обработка изображений: Пер. с англ. – М.: Мир, 1982. – Кн. 2. – 480 с.* ***7.*** *Бабак В. П. та ін. Обробка сигналів / В. П. Бабак, В. С. Хандецький, Е. Шрюфер – К: Либідь, 1996. – 392 с.*

УДК 004. 43(031)

ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ НАКОПИТЕЛЕЙ НА ЖЕСТКИХ МАГНИТНЫХ ДИСКАХ И БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Анна Страшина, Иван Четвериков
ВИТИ НТУУ «КПИ»

Аннотация: **Рассмотрен механизм автоматического скрытия дефектных секторов накопителей на жестких магнитных дисках в процессе их эксплуатации, создающий дополнительную угрозу безопасности современных информационных систем.**
Summary: **In this article was examinated mechanism of automatic latency of demage sectors ofmodern Hard Disk Drive during exploitation, wich making additional that to safety in information system.**
Ключевые слова: **Накопитель на жестких магнитных дисках, скрытие дефектов, информационные системы, безопасность**.

I Введение

История развития и совершенствования технических средств передачи, обработки и хранения информации показывает, что внедрение технических усовершенствований часто сопровождается появлением новых каналов утечки информации и, как следствие – возникновением новых угроз безопасности информации. В настоящее время огромное внимание уделяется теоретическим и практическим аспектам защиты информации в каналах передачи цифровых данных на основе новых сетевых технологий и телекоммуникаций, уязвимость которых вполне очевидна. Вместе с тем не следует забывать и о возможности появления новых угроз безопасности информации в процессе совершенствования даже тех элементов информационно-вычислительных систем, которые напрямую никак не связаны с каналами передачи информации.

II Основная часть

Одним из элементов, который широко используется в современных информационно-вычислительных системах, основанных на использовании персональных компьютеров, рабочих станций, информационных серверов и т. д., являются накопители данных на жестких магнитных дисках (винчестеры). Ведущая роль этих устройств в качестве основных элементов внешней памяти в современных информационно-вычислительных системах объясняется уникальным сочетанием их технико-экономических показателей, основными из которых являются [1]:

- емкость, определяющая количество (объем) хранимой информации;
- быстродействие, которое в значительной мере определяет производительность вычислительных систем в целом;
- стоимость хранения единицы информации.

Емкость современных серийно выпускаемых накопителей уже достигла значений в сотни Гигабайт и имеет устойчивую тенденцию к ежегодному удвоению [2]. Среднее время доступа к данным составляет единицы миллисекунд, а скорость передачи информации – десятки Мегабайт в секунду, что в основном удовлетворяет современные потребности обработки данных. Стоимость хранения единицы информации на винчестерах является самой низкой по отношению к возможным альтернативным способам хранения больших объемов информации.

Вместе с тем постоянное повышение качественных показателей винчестеров и естественным образом связанное с этим усложнение конструкций элементов трактов записи и чтения данных вынуждает производителей принимать специальные меры и реализовывать различные способы по обеспечению гарантированной надежности хранения данных, которая характеризуется следующими основными показателями [1]:

- вероятностью появления неисправимых ошибок (не более 10 – 14);
- вероятностью появления исправимых ошибок (не более 10 – 11);
- вероятностью ошибки поиска заданного сектора (не более 10 – 8).

Одной их причин, вынуждающих производителей принимать дополнительные меры по обеспечению надежности хранения данных в условиях постоянного роста плотности записи данных на диски является наличие неизбежных технологических погрешностей изготовления рабочих слоев дисков, приводящих к появлению участков дисков, на которых надежная запись и чтение данных становятся невозможными либо сразу после их изготовления, либо с течением времени. Поэтому для надежного хранения данных запись данных на такие участки дисков исключается за счет использования так называемых *механизмов (технологий) скрытия дефектов*. Такие механизмы используются как для исключения дефектных участков поверхностей дисков, выявленных на этапе заводского тестирования накопителей, так и для скрытия дефектных участков, возникающих в процессе эксплуатации накопителей. Сам термин "*скрытие*" отражает то обстоятельство, что результат работы этих механизмов, а иногда и сам факт их работы, скрыты от пользователя и никак не отражаются, например, на емкости накопителя (хотя в некоторых случаях могут отражаться на быстродействии). Для пояснения сущности этих механизмов кратко рассмотрим некоторые детали, касающиеся физической организации хранения данных на жестких магнитных дисках и доступа к ним [1].

Основной ячейкой хранения информации на диске является *физический сектор (Sector)*, который обычно обеспечивает хранение 512 байт данных. Физический сектор имеет определенную структуру, образуемую полями данных и рядом служебных полей сектора. Сектора располагаются последовательно вдоль концентрических окружностей, образуя дорожки (треки). Каждый сектор на дорожке имеет свой номер, а число секторов, размещаемых на каждой дорожке, зависит от ее радиуса (увеличивается по мере увеличения радиуса дорожки). При этом число секторов возрастает не непрерывно, а дискретно таким образом, что некоторое число расположенных рядом дорожек содержат одинаковое число секторов, образуя *зону* дорожек. Поэтому число секторов изменяется от зоны к зоне. Каждая зона может состоять из нескольких тысяч дорожек и содержать несколько сот секторов на одной дорожке. Рабочие магнитные слои могут размещаться на обеих поверхностях дисков, а сам накопитель может иметь несколько таких дисков, насаженнных на ось шпиндельного двигателя привода вращения дисков. Тогда совокупности дорожек одинаковых радиусов, расположенных на всех рабочих поверхностях дисков, образуют *цилиндры (Cylinder)*, число которых равно числу дорожек на одной поверхности. Соответственно, число всех дорожек будет равно числу цилиндров, умноженному на общее число рабочих поверхностей дисков. Поскольку каждой поверхности соответствует своя *головка записи/чтения (Head)*, то число всех дорожек можно определить и как произведение числа цилиндров на число головок. Отсюда вытекает способ однозначного задания внутренних (физических) координат секторов, заключающийся в указании для каждого сектора номера цилиндра (Cylinder), номера головки (Head) и номера сектора на дорожке цилиндра (Sector), называемый *CHS-адресом* сектора. Все физические сектора, размещаемые на рабочих поверхностях дисков, разбиваются на три области:

- *область данных пользователя;*
- *область служебных данных;*
- *резервная область.*

Именно *область данных пользователя*, как и следует из ее названия, предназначена для хранения полезной информации, а число секторов, образующих эту область определяет так называемую *форматированную емкость* накопителя. *Область служебных данных* предназначена для хранения служебной информации, необходимой для обеспечения работы самого накопителя, а *резервная область* предназначена для замещения дефектных секторов области данных пользователя, обнаруживаемых как при заводском тестировании, так и в процессе эксплуатации.

Доступ к секторам накопителей для выполнения операций записи/чтения осуществляется только через *внешний интерфейс накопителя* с использованием *интерфейсных команд*, состав и порядок использования которых определяется стандартами (спецификациями) на эти интерфейсы. При этом имеются существенные различия в порядке доступа к секторам области данных пользователя, области служебных данных и резервной области.

Доступ к секторам области данных пользователя осуществляется с использованием только обязательного набора команд, одинакового для накопителей любых производителей (в рамках поддерживаемого

интерфейса). Для обращения к секторам области данных интерфейсные команды используют внешние или *логические адреса* секторов. В настоящее время для логической адресации секторов используется линейная адресация (LBA – Logic Block Address), в соответствии с которой всем секторам области данных пользователя присваиваются непрерывно возрастающие номера LBA, начиная с LBA=0. Именно число логически адресуемых секторов, образующих область (зону) данных пользователя, и определяет форматированную емкость накопителя. Однозначное преобразование внешних логических (LBA) адресов секторов во внутренние физические (CHS) адреса осуществляется контроллерами накопителей при обработке интерфейсных команд с использованием специальных программ и таблиц трансляции адресов (*трансляторов*).

Структура, содержание и порядок доступа к секторам служебных зон накопителя не стандартизованы и определяются каждым производителем самостоятельно с использованием своих специфических интерфейсных команд (команд производителя), наличие (но не смысловое содержание) которых всегда предусматривается в спецификациях интерфейсов.

Произвольный доступ к секторам резервной области через внешний интерфейс накопителей вообще не предусмотрен. Физический сектор резервной области становится доступным только тогда, когда он использован для замены дефектного сектора области данных пользователя и включен в список логически адресуемых секторов под тем же логическим адресом, который имел исключенный сектор. При этом исключенный сектор вносится в список дефектных секторов (*список дефектов*), который записывается в служебную область накопителя и используется для установления однозначного соответствия между логическими (LBA) и физическими (CHS) адресами секторов, а доступ к исключенному сектору становится невозможным.

Физические сектора всех областей создаются в процессе *низкоуровневого форматирования*, выполняемого в заводских условиях одновременно с записью на поверхности дисков *сервоинформации*, необходимой для функционирования сервопривода системы позиционирования головок. После выполнения этих операций производится тестирование всех сформированных секторов на выполнение операций записи/чтения, формируется первоначальный список дефектов (Primary List, или P-List) и осуществляется скрытие обнаруженных дефектных секторов. С точки зрения защиты информации этот этап не представляет никакого интереса, поскольку является одним из этапов технологического процесса производства накопителей на жестких магнитных дисках.

Основной интерес с точки зрения безопасности информационных систем представляет реализация в современных накопителях механизмов (технологий) *автоматического скрытия дефектов в процессе эксплуатации.* Основной причиной внедрения таких механизмов явилось отмеченное выше стремление производителей обеспечить требуемые уровни надежности хранения данных на накопителях в целом в условиях постоянного возрастания поверхностной плотности записи данных на диски и связанного с этим снижения надежности хранения данных в каждом отдельном секторе в процессе эксплуатации накопителей. Побочным же результатом внедрения механизмов автоматического скрытия дефектов является то, что функционирование этих механизмов создает предпосылки (техническую основу) для существования специфического канала утечки конфиденциальной информации, связанного с возможностью неконтролируемого накопления данных в скрытых секторах накопителя и последующего извлечения этих данных.

В накопителях различных моделей могут встречаться различные способы реализации механизмов автоматического скрытия дефектов, отличающиеся:

- критериями (правилами) принятия решений на включение того или иного сектора в список дефектных секторов;
- способами замены дефектных секторов области данных на сектора резервной зоны с сохранением прежних логических адресов.
- способами размещения участков резервной области по поверхностям дисков.

Информация о деталях реализации механизмов автоматического скрытия дефектов является интеллектуальной собственностью производителей накопителей на жестких дисках и в открытых источниках практически отсутствует. В технической документации производителей (см., например [4]) указывается как правило лишь сам факт (иногда название) таких механизмов и технологий. Однако в некоторых источниках указывается на существование двух основных способов автоматической замены дефектных секторов [5]:

- способ переназначения (подстановки), при котором вместо дефектного сектора назначается другой сектор из резервной зоны, которая может находиться в любом месте диска;
- способ пропуска, при котором вместо дефектного сектора назначается очередной в порядке следования физический сектор, данные из которого (и всех последующих до конца дорожки) сдвигаются в сторону резервной области в конце дорожки.

Каждый из этих способов имеет свои достоинства и недостатки. В принципе возможно и комбинированное использование обоих этих способов в одном накопителе. Отмечается также, что автоматическое скрытие дефектов может осуществляться либо на основе результатов автоматического сканирования поверхностей в свободное от дисковых операций время, либо непосредственно в процессе выполнения операций чтения/записи [4, 5].

Однако, вне зависимости от способа реализации сущность скрытия дефектов заключается в том, что логический адрес дефектного сектора, т. е. адрес, который используется в командах внешнего интерфейса для обращения к секторам накопителя, отождествляется с другим физическим сектором, расположенным в резервной области, а дефектный сектор исключается из списка логически адресуемых секторов и становится недоступным через внешний интерфейс накопителя. Технически это осуществляется путем формирования растущего списка дефектов (Grown List, или G-List) и корректировки таблиц трансляторов накопителей, с помощью которых логические адреса секторов, указываемые в командах обращения к секторам, преобразуются в физические координаты секторов на рабочих поверхностях дисков. В результате данные пользователя, хранившиеся в скрытых физических секторах, становятся недоступными для записи/чтения через внешний интерфейс накопителя любыми программными средствами, использующими обязательный набор команд, определяемый стандартами (спецификациями) на интерфейсы накопителей. Важным, при этом, является то обстоятельство, что данные, накопленные в скрытых секторах, могут, во-первых, сохраняться и после вывода накопителя из эксплуатации по различным причинам, а во-вторых, существует техническая возможность извлечения этих данных на любом этапе жизненного цикла накопителя [3]. Эти обстоятельства и определяют, таким образом, возможность существования специфического канала утечки информации с накопителей на жестких магнитных дисках, связанного с функционированием *механизма автоматического скрытия дефектных секторов.*

Возможность извлечения данных из скрытых секторов накопителей может быть реализована путем очистки таблиц дефектов G-List и последующего пересчета таблиц трансляторов накопителей, в результате чего скрытые ранее сектора с накопленными данными могут снова стать доступными для чтения/записи через внешний интерфейс накопителя. Такая возможность может быть реализована с помощью специальных программных и аппаратно-программных средств, использующих для доступа к служебным зонам накопителей недокументированные наборы команд производителей, не входящие в перечень обязательных команд спецификаций внешних интерфейсов. Учитывая, что различные производители используют свои и отличающиеся друг от друга наборы команд доступа к служебным зонам, такие средства могут быть только специализированными, т. е. предназначенными для работы только с накопителями конкретных моделей.

III Выводы

Наличие в современных накопителях на жестких магнитных дисках механизмов автоматического скрытия дефектов, связанная с этим возможность неконтролируемого накопления информации в скрытых секторах накопителей и возможность ее извлечения специальными средствами, требуют тщательного анализа всех организационно-технических мероприятий по защите информации в информационно-вычислительных системах с точки зрения полноты учета указанных особенностей и, возможно, разработки дополнительных мер по предотвращению утечки конфиденциальной информации с накопителей на жестких магнитных дисках, используемых в этих системах.

Литература. ***1.*** *Дисковая подсистема ПК/М. Гук. – СПб.: Питер, 2001. – 336 с.* ***2.*** *The future of magnetic data storage technology/ D. A. Thompson, J. S. Best. – IBM Journal Research Development, Vol. 44, No. 3 May 2000, p. 311-322.* ***3.*** *Аппаратные методы восстановления информации, хранимой на жестких дисках/ С. Р.Коженевский – "Реєстрація, зберігання і обробка даних. Том 4, № 2, 2002 р. стр. 62-71.* ***4.*** *WD Caviar AC12100/AC23200/AC24300/AC35100/AC36400. Technical Reference Manual. Western Digital Corporation, 1997, – 86 с.* ***5.*** *Современные накопители на жестких магнитных дисках (часть 1)/ В. Морозов, С.. Яценко. – "Ремонт электронной техники" № 3, 2003, стр. 34-39.*