ставшем неисправным НЖМД. Более того, при неисправности элементов, расположенных в камере накопителя даже в условиях специализированного сервисного центра невозможно гарантировать, что в процессе ремонта сохранится исходное расположение головок. Поэтому за исключением простейших случаев (отказ контроллера диска) при выходе накопителя из строя гарантированно уничтожить информацию можно только разрушающими методами.

Опыт фирмы ЕПОС по ремонту жестких дисков и восстановлению информации позволил создать стенд для технического обслуживания жестких дисков (рис. 3).

Рисунок 3 – Стенд для технического обслуживания жестких дисков

Стенд позволяет осуществить полную диагностику жесткого диска, адаптивное копирование дисков (даже при некоторых повреждениях диска – источника), а также гарантированное уничтожение информации путем многократной записи специальных кодов во все физические сектора жесткого диска.

В настоящее время в ООО «ЭПОС» проводится ОКР по подготовке к серийному производству следующего поколения стенда для технического обслуживания накопителей на жестких дисках, имеющего расширенные функции как по диагностике накопителя, так и по уничтожению информации. В частности, для уничтожения информации на дисках, имеющих значительные повреждения, стенд комплектуется устройством, позволяющим стирать данные на всем диске, включая служебные области и сервометки, путем воздействия мощного магнитного импульса.

УДК 681.3.06

ЗАЩИТА ДАННЫХ НА КОМПАКТ-ДИСКАХ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

Виталий Носов, Александр Манжай

Национальный университет внутренних дел, г. Харьков

Анотація: **Проведено аналіз відомих принципів захисту даних на компакт-дисках від несанкціонованого копіювання. Розглянуто новий метод, що забезпечує більш високий ступінь захисту від копіювання.**

Summary: **The analysis of known principles of the data protection on compact discs from the non-authorized copying is carried out. The new method providing the big degree of protection against copying is considered.**

Ключевые слова: **Защита данных, несанкционированное копирование, компакт-диск.**

I Введение

В условиях стремительного развития компьютерной техники остро встала проблема защиты интеллектуальной собственности, носителем которой, прежде всего, являются компакт-диски (CD). В настоящее время со стороны компаний-производителей программного обеспечения и мультимедийных CD активизирована борьба с незаконным копированием и тиражированием таких компакт-дисков. Однако эффективных результатов она пока не приносит, что связано с необходимостью постоянного поиска новых и совершенствования существующих методов защиты компакт-дисков от несанкционированного копирования.

В общем случае система защиты CD представляет собой комплекс средств, предназначенный для затруднения (в идеале – предотвращения) нелегального копирования (исполнения) защищаемого программного модуля, с которым она ассоциирована.

В настоящее время уже устоявшейся можно считать структуру системы защиты CD, которая

определяется следующими основными требованиями:

- выявлять факт несанкционированного запуска программы;
- реагировать на факт несанкционированного запуска программы;
- противодействовать возможным атакам злоумышленника [1].

На сегодняшний день известно несколько принципов защиты CD, многие из которых уже преодолены "взломщиками". Рассмотрим наиболее распространенные методы защиты.

II Анализ известных методов защиты

Разработчики, как правило, умалчивают о принципах работы своих программ защиты, поэтому приходится довольствоваться скудной информацией с рекламных сайтов фирм, специализирующихся на защите CD, а также «передовым опытом современных хакеров».

Все методы защиты CD можно условно разделить на защиту данных, записанных на:

– программные CD;
– мультимедийные (музыка, игры, видео) CD.

Принципы защиты данных, разработанные для мультимедийных CD, как правило, применимы и для программных, поэтому такие принципы защиты можно назвать универсальными. Сама защита может быть реализована с целью:

– предотвращения несанкционированного копирования (НСК) на жесткий диск;
– предотвращения НСК на другой CD;
– предотвращения НСК на жесткий диск и другой CD (комбинированная защита).

Таким образом, основные принципы защиты CD можно представить в виде следующей схемы (рис. 1).

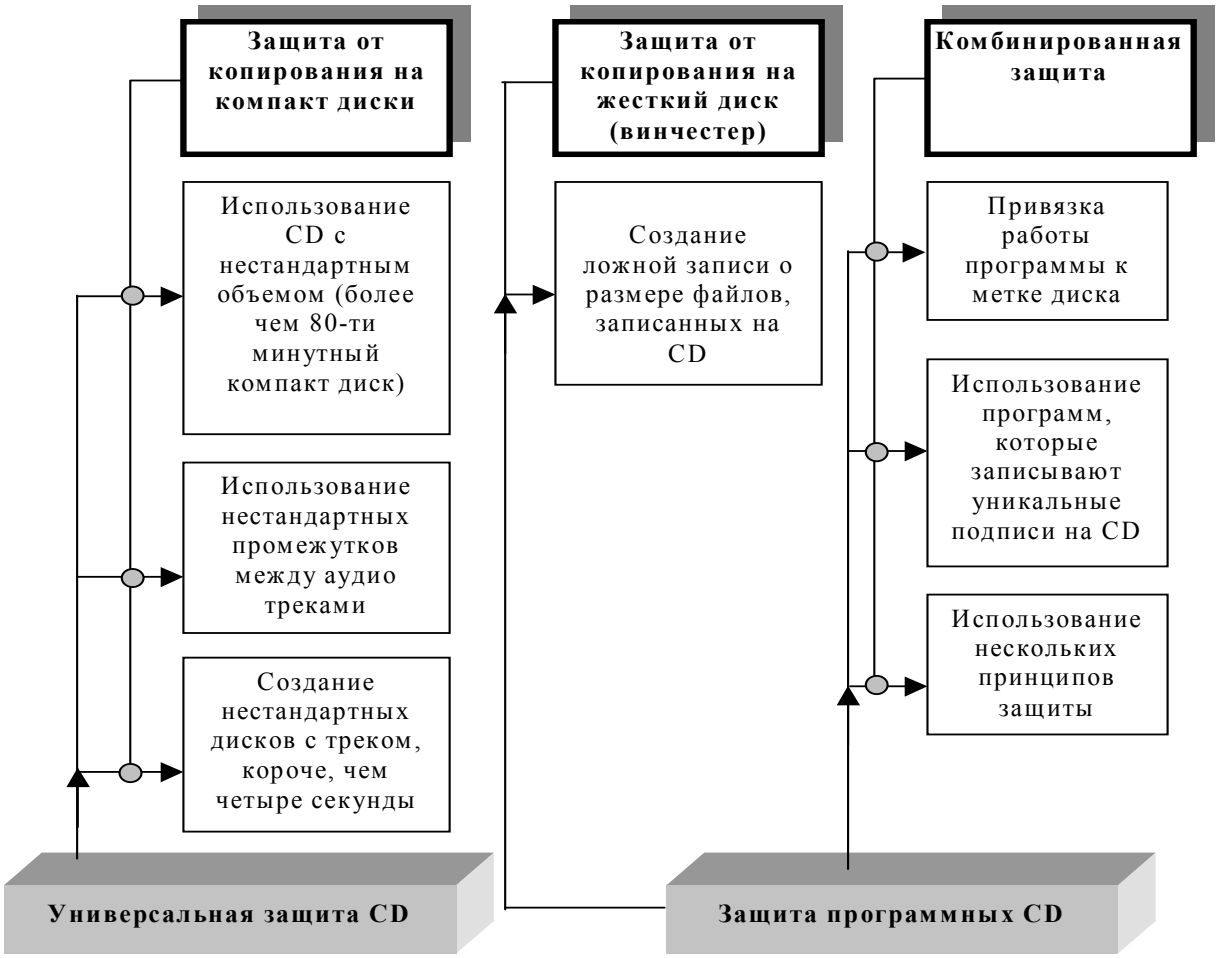

Рисунок 1 – Принципы защиты CD

Следует заметить, что защита CD от НСК, как правило, основывается на особой структуре данных, используемой для хранения информации, либо на привязке к аппаратному обеспечению, в частности к приводу чтения CD-ROM.

Кратко проанализируем основные известные методы защиты (рис. 1).

1) Использование CD с нестандартным объемом данных (более чем 80-ти минутный компакт-диск).

Данный метод реализуется путем заполнения заготовки диска до тех пор, пока это позволяет привод. Иными словами, происходит «пережигание» диска, вследствие чего его объем, как правило, становится на несколько минут больше, что приводит в большинстве случаев к невозможности копирования такого CD.

Достоинства: для преодоления такого метода защиты необходимы специальные диски или приводы, что делает этот способ малопривлекательным для атаки злоумышленников с точки зрения материальных затрат.

Недостатки: во-первых, этот метод является довольно дорогим, что делает его неприемлемым для некоторых собственников интеллектуальной продукции; во-вторых, использование таких дисков может повлечь их нечитаемость некоторыми приводами CD-ROM.

2) Создание ложной записи о размере файлов, записанных на CD.

Это производится установкой размера файла большим, чем есть на самом деле в образе диска (файл образа диска, в данном случае, создается перед записью данных на CD и является виртуальным диском, в котором возможно изменить некоторые параметры). При ложной записи размера файла происходит как бы наложение одних данных на другие, но поскольку защищаемой программе известны реальные размеры файлов, то она будет работать корректно.

Для этих целей целесообразно брать файл с данными, без которого программа работать не будет (например *.dat) и его размер фиктивно делать равным порядка 800 и более Мбайт. Некоторые exe-файлы считают свою контрольную сумму, поэтому их в данном случае использовать нельзя.

Достоинства: диск, защищенный таким образом, записать на винчестер не удается, по крайней мере, тот файл, размер которого виртуально делается фиктивно большим.

Недостатки: эта защита обычно не работает при клонировании диска, то есть создании его образа специальными утилитами. К тому же отсутствует стандартное программное обеспечение для создания таких дисков.

3) Использование нестандартных промежутков между аудио треками.

Существует два основных способа записи на CD рекордерами – disc-at-once (DAO) и track-at-once (TAO).

В режиме DAO (диск за один раз) записывается весь CD за один подход, при этом, возможно записать множество треков. Вся запись должна завершиться без прерываний, и добавить на диск информацию нельзя (треки или дорожки – участки записи, расположенные по спирали). Треки могут быть аудио и dat (для хранения данных).

Режим TAO (потрековая запись) позволяет осуществлять запись в несколько подходов. Существует минимальная длина трека, составляющая 600 кБ (300 блоков или 4 с) для стандартного CD с данными, и максимальное количество треков – 99 на диск, кроме того, некоторое пространство диска затрачивается при включении и выключении лазера.

Поскольку лазер выключается и включается на каждом треке, рекордер оставляет несколько блоков между треками, которые называются выводящими (run-out) и вводными (run-in) блоками, они предназначены для связывания дорожек между собой. Если все сделано правильно, то эти блоки бесшумны и, обычно, незаметны при воспроизведении. Стандартный промежуток между аудио треками составляет 2 с (150 блоков) и автоматически записывается в режиме track-at-once.

Таким образом, устанавливая нестандартный размер промежутков между треками при записи данных на CD, возможно заблокировать процесс перезаписи рекордером таких данных на другой диск в режиме track-at-once.

Некоторые приводы и/или программные пакеты не позволяют регулировать размер промежутков между треками при записи в режиме track-at-once, и устанавливают двухсекундные промежутки, даже если в оригинале их не было.

Достоинства: эти диски не копируются распространенными программами и рекордерами.

Недостатки: в режиме disc-at-once возможно копирование таких дисков.

4) Создание нестандартных дисков с треком, короче, чем четыре секунды.

При записи данных на CD программой записи создается специальный CUE-файл, который определяет режим, вид и порядок записи данных.

Защита основана на записи в CUE-файл вместе со значащими треками фиктивных аудио треков и треков данных как можно меньшей длины, в которых ничего не записывается или записывается всякий "мусор". Защищенное таким образом приложение должно проверять наличие и размер таких треков.

Достоинства: создание такого диска приводит к тому, что большинство программ для записи/копирования CD не могут продублировать диск с такой защитой. Следует отметить, что создание трека длиной около одной секунды вообще не позволяет копировать диск ни одному известному рекордеру. Перемешивание таких аудио треков с треками данных ставит в тупик некоторые дупликаторы дисков.

Недостатки: содержимое диска в основном копируется на жесткий диск и работает с него, если не предусмотрена дополнительная защита.

5) Привязка работы программы к метке диска.

Одна из самых простых проверок – это сравнение метки имени диска с оригиналом. Метка имени диска может создаваться, используя нестандартные символы ASCII. Такой метод относится к так называемым простейшим видам защит.

Достоинства: простота реализации.

Недостатки: такая защита малоэффективна, поскольку не защищает от дупликаторов дисков и от квалифицированных пользователей, которым ничто не мешает создать такую же метку на копии диска.

6) Использование программ, которые записывают уникальные подписи в CD.

Утверждается [3], что эти подписи обнаруживаются всеми приводами CD-ROM, но не воспроизводятся без специального оборудования. Программа не запускается в случае отсутствия подписи. Механизм записи таких подписей не раскрывается.

Достоинства: большинство программ для записи/копирования CD не могут продублировать диск с такой защитой.

Недостатки: некоторые программы клонирования способны копировать большинство таких дисков при условии правильного сочетания считывающего и записывающего устройств.

7) Использование нескольких принципов защиты.

Предполагает реализацию универсального метода (рис. 1), способного наиболее эффективно решить задачу защиты данных на CD.

Достоинства: эффективность работы.

Недостатки: зависят от выбранных принципов работы.

III Предлагаемый метод защиты

Этот метод основывается не только на свойствах самого диска, но и на свойствах аппаратного обеспечения ЭВМ.

Метод включает в себя два уровня.

1. Запись в CUE-файл фиктивных треков аудио и данных размером менее 4 с.

Этот элемент защиты необходим для того, чтобы обезопасить исходный диск от копирования на другой CD. Именно на CD, потому что, как отмечалось ранее, защищенный таким способом диск сравнительно легко скопировать на жесткий диск.

2. Привязка к устройству чтения CD-ROM.

Этот элемент необходим для того, чтобы обеспечить защиту от эмулирования диска программами создания его прообраза или простого копирования на жесткий диск.

Поясним суть защиты второго уровня.

Известно [2], что скорость передачи данных с жесткого диска намного больше скорости передачи данных с CD:

$$V_{CDf} < V_{HDD}, \quad (1)$$

где V_{CDf} – фактическая скорость передачи данных с компакт диска;

V_{HDD} – скорость передачи данных с жесткого диска.

Можно говорить о номинальной (заявленной) и фактической скорости передачи данных с компакт-дисков. Отметим, что ситуация, когда фактическая скорость передачи данных с диска равна номинальной скорости передачи данных привода, теоретически возможна, однако на практике недостижима в условиях плохо отцентрированных дисков, используемых в отечественной промышленности, а также неравномерности чтения с их поверхности.

Второй уровень защиты начинает работать, когда защищенная программа запускается на выполнение. Специальная процедура при этом вычисляет параметры V_{CDf} и V_{HDD}, и в случае их удовлетворения неравенству (1) допускает защищаемый файл (файлы) на выполнение.

Заданные проверки необходимо внедрить непосредственно в исполняемые файлы, подлежащие защите.

Для нахождения V_{CDf} целесообразно использовать следующий прием. Необходимо измерить время считывания файла t_r фиксированного размера S_c, а затем найти фактическую скорость передачи данных конкретного привода чтения CD $V_{CDf}=S_c/t_r$.

Максимальная скорость передачи данных жесткого диска определяется по формуле [2]:

$$MDTR = SRT \cdot 512 \cdot RPM/60 \text{ (байт/с)}, \quad (2)$$

где SRT – количество секторов на дорожке;

RPM – скорость вращения дисков (об/мин).

Для удобства расчетов создается файл размером, кратным скорости устройства чтения CD-ROM (1x=150 кБ/с). В программе защиты дополнительно необходима проверка размера этого файла для исключения возможности взлома программы путем тривиального изменения размера файла. Следующим шагом записывается этот файл в конец компакт-диска, с целью его максимально быстрого считывания, хотя это не является обязательным условием. Затем, используя отношение размера файла ко времени его считывания, находится V_{CDf}. Скорость передачи данных с жесткого диска V_{HDD} принимается постоянной и равной MDTR для наиболее распространенного типа жесткого диска. Найденные V_{CDf} и принятое V_{HDD} используются для проверки неравенства (1).

В настоящее время на кафедре "Защиты информации и специальной техники" НУВД проводится совершенствование и реализация изложенного метода для защиты данных, являющихся интеллектуальной собственностью и записанных на компакт-диски.

Литература: 1. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов/ П. Ю. Белкин, О. О. Михальский, А. С. Першаков и др. – М.: Радио и связь, 1999. – 168 с. 2. Аппаратные средства PC. – 4-е изд., перераб. и доп. – /Колесниченко О. В., Шишигин И. В. – СПб.: БХВ-Петербург, 2001. – 1024 с. 3. TTR Technology – DiscGuard (http://www.ttr.co.il/)

УДК 004.085.2

ФИЗИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ КОМПАКТ-ДИСКОВ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

Вячеслав Петров, Андрей Крючин, Семен Шанойло, Игорь Косяк, Олег Цубин

Институт проблем регистрации информации НАН Украины

Аннотация: **Рассмотрено применение физических методов защиты компакт-дисков от копирования. Приведена информация о созданном аппаратно-программном комплексе нанесения графической информации на штампы для тиражирования компакт-дисков.**

Summary: **The application of physical methods of CD protection from copying is considered. The information on the created hardware-software complex for recording of the graphic information on the stamps for CD duplication is presented.**

Ключевые слова: **Компакт-диск, графический элемент.**

Введение

Компакт-диски, как средство массового распространения компьютерной информации, являются объектом, который требует многоуровневой защиты от несанкционированного копирования записанной информации. Несанкционированное копирование компакт-дисков является грубым нарушением авторских прав разработчиков программных продуктов, авторов и исполнителей музыкальных произведений. Доступность средств записи информации на компакт-диски, уменьшение стоимости CD-R делают задачу защиты компакт-дисков от копирования особенно актуальной.

Анализ методов защиты компакт-дисков от несанкционированного копирования

Методы защиты от копирования можно разделить на две группы: методы программной защиты [1, 2] и методы физической защиты [3, 4]. В принципе методы программной защиты должны обеспечивать невозможность копирования записей с компакт-диска на компакт-диск или винчестер. Такие разработки проводятся рядом фирм как за рубежом, так и в Украине [1, 2]. Наиболее известные разработки систем программной защиты выполнены следующими зарубежными компаниями:

- Macrovision (программа Safe Disc и ее обновление Safe Disc V2) – http://www.macrovision.com;
- Sony (SecuROM) – http://www.secuROM.com;
- Link Data Security (программа Cop's Copylock);
- VOB (программа Protect CD);
- MLS Laser Lock International (программа Laser Lock) – http://www.laserlock.com. [4] и др.

Украинскими разработчиками программных методов защиты (фирма "Bua 4C") предлагаются следующие