підтримує стандартні протоколи взаємодії з більшістю видів телекомунікаційних мереж (телефонних, Інтернет, IP-телефонії, ISDN, IN, Frame Relay, ATM, стільникового зв'язку тощо);

надає будь-яку інформацію в межах предметного застосування, на яке він налаштований;

забезпечує незалежність використаних програмно-апаратних рішень від галузі призначення контакт-центру.

Сьогодні пропонується широкий вибір продуктів, призначених для побудови контакт-центрів і їх кількість стрімко зростає.

Вищезазначене дозволяє на базі контакт-центру створювати економічно ефективні рішення, у т. ч. і в сфері керування комплексними системами ТЗІ у розподілених ІС.

IV Висновки

1. На базі програмно-апаратних платформ центрів обслуговування телефонних викликів у багатьох практично важливих застосуваннях можлива економічно обгрунтована побудова центрів керування територіально розподіленими ІС, включаючи побудову підсистем керування комплексними системами ТЗІ.

2. Як канали транспортування технологічної інформації в централізованих системах керування, створюваних на основі ЦОВ, можливо і у багатьох випадках доцільно застосувати стандартні комутовані канали телефонної мережі загального використання. Це спрощує і здешевлює побудову систем керування, а також підвищує захищеність технологічної інформації, що в них циркулює.

3. Шляхом підключення аналогових портів ЦОВ та/або пристроїв віддаленого контролю до різних територіально рознесених АТС забезпечується можливість економічно ефективного внесення апаратної надлишковості з метою адаптивного перерозподілу ресурсів в задачах керування засобами ТЗІ.

4. Для побудови систем централізованого керування складними ІС, створеними на основі гетерогенних мереж, доцільно використовувати мультимедійні програмно-апаратні пристрої обслуговування викликів (так звані контакт-центри).

Література: ***1****. William C. Goers, Michael R. Brenner. Implementing a Management System Architecture Framework / Bell Labs Technical Journal. – October-December, 2000. – 31-43 p.* ***2.*** *International Telecommunication Union, Rec. M.3010. Principles for a Telecommunications Management Network (TMN). – May,1996.* ***3****. Tele-Management Forum, Document GB910, Version 2.1. Telecom Operations Map. – Mart, 2000.*

УДК 004.056.53

ОБ ОДНОМ ПОДХОДЕ К ПОСТРОЕНИЮ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ НА КОМПАКТ-ДИСКАХ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ

Виталий Носов, Александр Манжай

Национальный университет внутренних дел, г. Харьков

Анотація: **Пропонується один з підходів до побудови системи захисту компакт-дисків від несанкціонованого копіювання.**

Summary: **One of the approaches to construction the compact discs protection system against the non-authorized copying is offered.**

Ключевые слова: **Система защиты, несанкционированное копирование, компакт-диск.**

I Введение

На современном этапе развития общества, когда информационные отношения формируют, по сути, новую сферу экономики, становится актуальным вопрос об эффективной системе защиты права собственности на информацию.

Принятие в 2001 г. нового Уголовного кодекса Украины стало в нашей стране важным этапом в борьбе с компьютерными преступлениями. Правоохранительными органами был проведен ряд мероприятий по предупреждению, раскрытию и расследованию такого рода преступлений. Однако принятые меры носят, как правило, административный характер, что не позволяет достаточно эффективно противостоять киберпреступности. Вместе с тем кроме организационных мер целесообразно применять и так называемые программно-технические методы и средства защиты с целью повышения защищенности хранимой

информации. Применение таких методов защиты в большинстве случаев возложено на субъектов, заинтересованных в законном распространении принадлежащей им на правах собственности информации.

Частным случаем применения программно-технических методов защиты информации является защита данных на компакт-дисках от несанкционированного копирования с использованием программных средств. Заинтересованные лица вкладывают значительные средства в развитие и разработку новых технологий защиты в этой сфере, что свидетельствует об актуальности проблемы несанкционированного копирования (НСК) информации.

В частности, на сегодняшний день в некоторых легальных компаниях-производителях при разработке системы защиты прослеживается тенденция ухода от непосредственно программных к в большей мере физическим мерам защиты. Таким способом защиты, например, является создание специальных дисков, отличных от стандартных по своей структуре. Думается, что хотя данный способ защиты и является весьма надежным, однако его достоинства перекрываются такими недостатками:

- значительно повышается стоимость единицы продукции (компакт-диска с данными);
- уменьшается прибыль организации вследствие высокой себестоимости единицы продукции по сравнению с продукцией, защищенной программными методами;
- снижается конкурентоспособность;
- нарушается принцип универсальности и гибкости системы защиты в целом в результате ухода от принятых стандартов и т. д.

В [2] приводился перечень наиболее распространенных из ныне существующих способов защиты и предлагался иной, более совершенный, комбинированный метод защиты. Этот метод впоследствии был тщательно проанализирован, несколько изменен и дополнен, что позволило создать эффективную систему защиты (СЗ) от НСК. Меры, применяемые в предлагаемой СЗ, взаимодополняют, а в некоторых случаях подкрепляют друг друга.

II Предлагаемая система защиты

СЗ можно представить в виде трёх составляющих (рис. 1):

Рассмотрим по отдельности каждый элемент СЗ.

Рисунок 1 – Общий вид системы защиты CD от НСК

1. Защита от НСК на HDD.

Известно [1], что скорость передачи данных с жесткого диска намного больше скорости передачи данных с компакт-диска (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.

Первый 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.

Каждый компьютер имеет свои уникальные характеристики по считыванию данных с жесткого диска (HDD) и привода чтения компакт-дисков (CD-ROM). Поэтому целесообразно измерять параметры индивидуально для каждого ПК с последующей скрытной записью этих сведений в служебную часть данных

операционной системы (предварительно выгрузив из оперативной памяти посторонние резидентные программы).

Данные, по которым определяются скорости чтения с HDD и CD-ROM, целесообразно хранить на защищённом CD в виде файла фиксированного размера. Этот файл должен быть в процессе инсталляции переписан на жесткий диск с последующим измерением параметров HDD и сравнением их с параметрами считывания файла с CD.

При последующих запусках исполняемого файла (в котором встроена система защиты) с CD будет осуществляться проверка данных о скорости считывания CD в приводе CD-ROM с записанными в служебной области данными операционной системы.

2. Защита от НСК с одного компакт-диска на другой.

Прежде чем рассмотреть вторую ступень системы защиты напомним структуру компакт-диска.

В соответствии с принятыми стандартами поверхность диска разделена на три области (рис. 2):

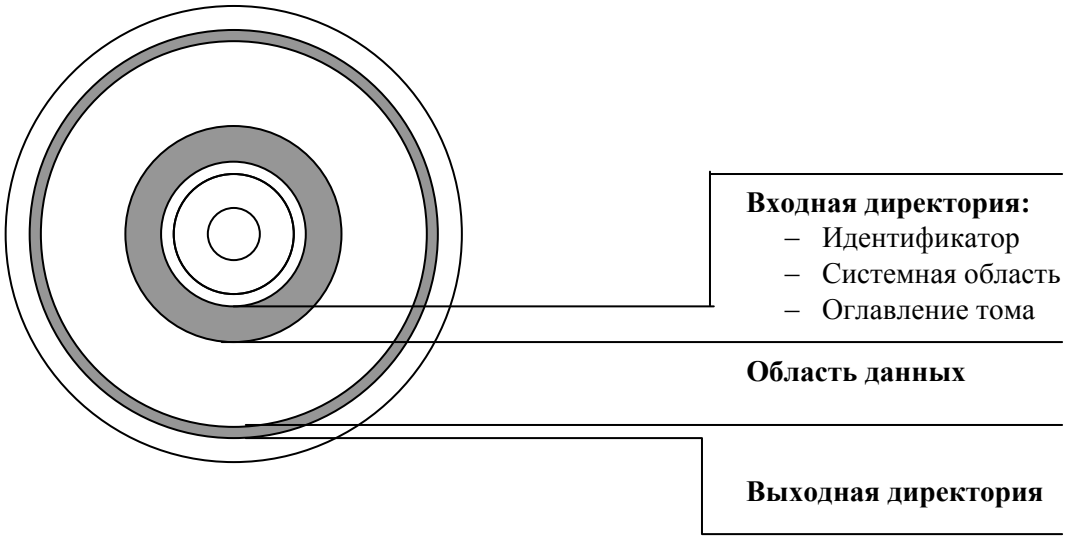

Рисунок 2 – Структура компакт-диска

– входная директория (Lead in) – область в форме кольца, ближайшего к центру диска (ширина кольца 4 мм); считывание информации с диска начинается именно с входной директории, где содержатся оглавление (Volume Table of Contents, VTOC), адреса записей, число заголовков, суммарное время записи (объем), название диска (Disc Label);

– область данных;

– выходная директория (Lead out) имеет метку конца диска.

Основным отличием структуры каталога компакт-диска от структуры каталога дискеты (или структуры каталога DOS) является то, что на CD в системной области записаны адреса файлов [1], причем размер области Lead in – 9 Мбайт (1 мин); а Lead out – 4,5 Мбайт (30 с).

Вторую ступень защиты можно представить в виде алгоритма приведенного на рис. 3:

Поясним приведенный алгоритм.

1. Создается образ записываемых данных, в которые включена кроме защищаемых данных и контрольного модуля некоторая гамма (G, последовательность бит информации), используемая в дальнейшем для генерации ключевой последовательности.

2. Записывается созданный образ на компакт-диск.

3. Производится физическое повреждение части секторов CD, причем уничтожаются те сектора, данные в которых не несут смысловой нагрузки. Такое повреждение можно реализовать, например, путем лазерного прожига (промышленные условия) или нанесением царапины на поверхность диска (непромышленные условия).

4. Специальная программа-генератор выполняет функцию Ф для создания ключа К. Аргументами функции Ф являются:

а) данные областей Lead in и Lead out, где R(Lead in) – определенные биты области Lead in, P(Lead out) – определенные биты области Lead out; C(…) – функция конкатенации полученных битов (воссоздание таких же (в том же месте на CD) областей на другом диске будет весьма проблемным);

б) функцией блок S, формируемый в результате анализа номеров и количества поврежденных секторов – меток, будет обрабатываться Ф с учетом кода ошибки, полученного при попытке чтения поврежденных секторов. Поскольку секторов на диске более 300000 [1], то воспроизведение меток такого же вида и на том же месте будет маловероятным.

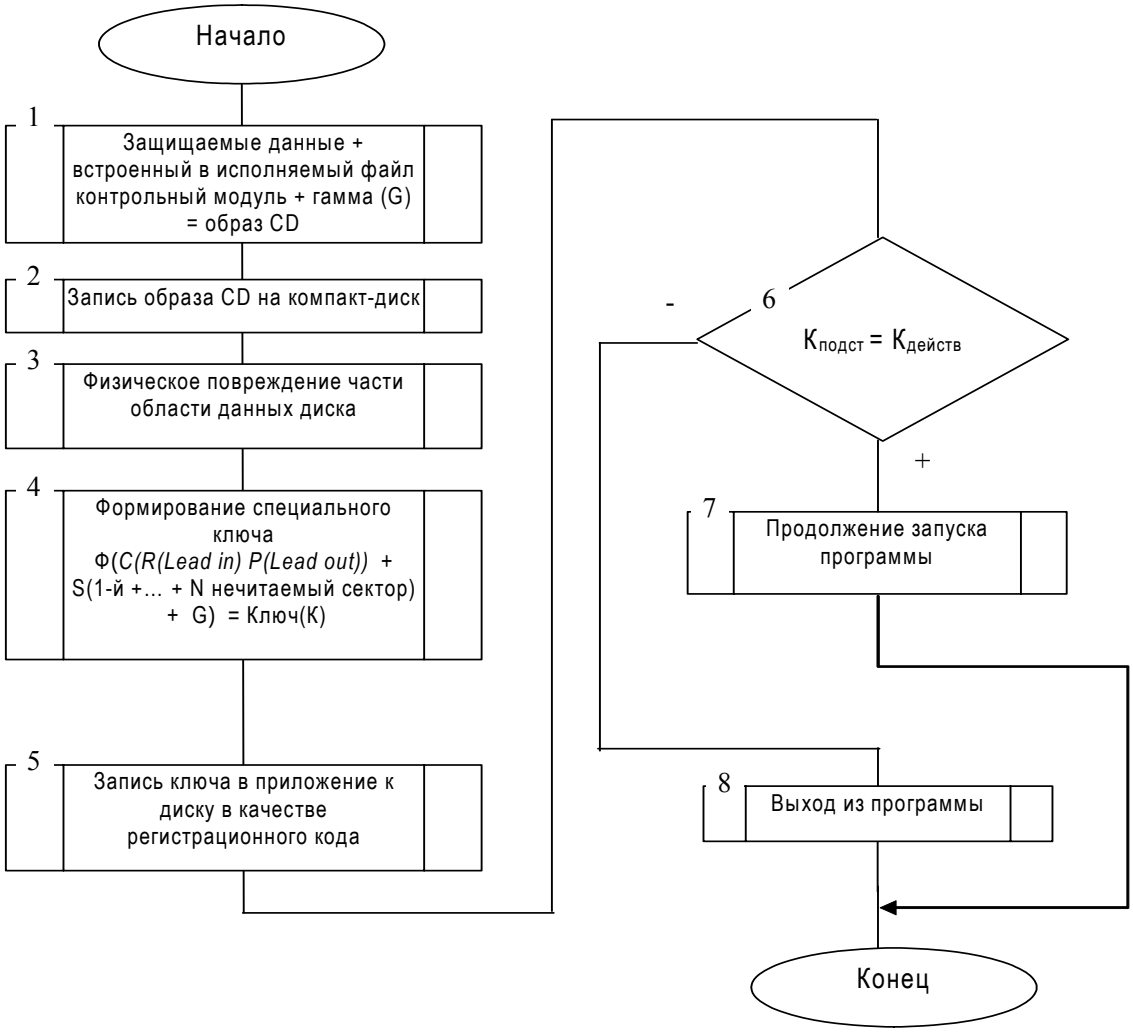

Рисунок 3 – Алгоритм осуществления второй ступени защиты

Изначально, помимо обработки кода ошибки выдаваемого при чтении поврежденного сектора, необходимо встроить в код программы защиты проверку наличия самих повреждений с целью повышения надежности защиты.

Для непромышленных условий создания СЗ стойкость этого этапа главным образом будет определяться секретностью алгоритма генерации ключевой последовательности.

В промышленных же условиях возможно повысить стойкость этого этапа СЗ путем предварительной закладки в код программы данных о поврежденных секторах с последующим лазерным уничтожением заданных секторов.

Вероятность воспроизведения нанесенных меток на CD можно оценить следующим образом. Данные на диске представлены в виде единственной спиральной дорожки с расстоянием 1,6 микрона между витками, что соответствует плотности дорожек 625 витков на миллиметр или 15875 витков на дюйм [3].

Для оценки введем следующие допущения относительно технических возможностей злоумышленника. Злоумышленник обладает «микроскопом» с разрешением один микрон и высокоточными (погрешность +1 сектор) инструментами нанесения меток.

Пусть на CD размещено N меток, каждая из которых может содержать несколько секторов. Тогда для данных условий вероятность совпадения нелегальной метки с легальной (Pm) будет равна 1/9 (рис. 4).

Соответственно вероятность воссоздания идентичных меток на всем диске (PCD), будет равна 1/9N. Причем, если отвести под систему меток 1% стандартного CD (700 Мб), с соотношением поврежденные/неповрежденные данные = 1/2, то вероятность PCD составит менее 1/91000;

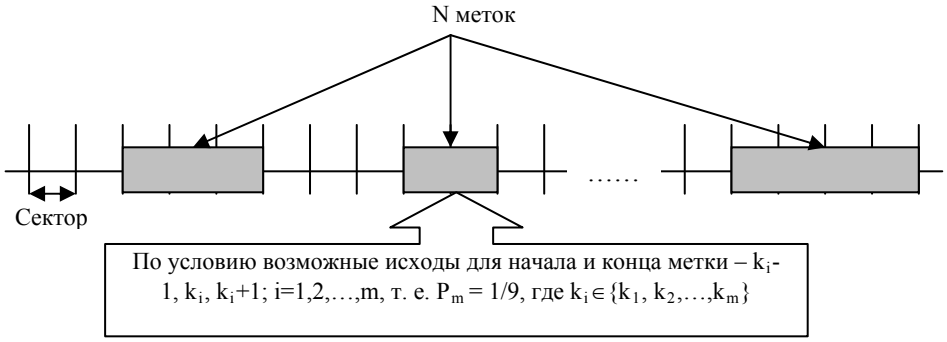

Рисунок 4 – Развернутый вид спиральной дорожки CD с нанесенными метками

в) гамма G. Главное требование к гамме состоит в том, что ее размер должен соответствовать размеру шифруемых данных.

5. Сгенерированный ключ записывается в приложение к защищенному диску (например, распечатка на обложке диска).

6. В момент запуска защищенного исполняемого файла осуществляется вывод запроса с предложением ввести ключ. Если этот ключ совпадет со сгенерированным контрольным модулем исполняемого файла (аналогично блоку (4)), то выполнится шаг 7, в противном случае – 8 (см. рис. 3).

3. Защита программного кода от НСК.

Реализацию данной ступени защиты следует проводить с учетом следующих требований:

1. *Защищенность от программ дизассемблеров;*
2. *Отслеживание работы отдельных распространенных отладчиков (Softice, WinDB) с последующей их выгрузкой из оперативной памяти либо противодействием их работе;*
3. *Противодействие трассировке;*
4. *Защищенность от программ-отладчиков;*
5. *Криптографическая защита кода программы;*
6. *Использование нестандартных методов упаковки;*
7. *Защищенность от специальных программ-резидентов;*
8. *Выгрузка опасных резидентов из памяти;*
9. *Использование недокументированных операций ввода-вывода;*
10. *Защищенность от иных программ, выступающих потенциальными источниками угрозы.*

III Заключение

На сегодняшний день кафедрой "Защиты информации и специальной техники" Национального университета внутренних дел проводится реализация вышеописанной системы защиты. Основная часть программного кода под OS Windows уже реализована и подтвердила свою работоспособность.

Литература: ***1.*** *Аппаратные средства PC. – 4-е изд., перераб. И доп. - /Колесниченко О. В., Шишигин И. В. – СПб.: БХВ-Петербург, 2001. – 1024 с.* ***2.*** *Носов В. В., Манжай А. В. Защита данных на компакт-дисках от несанкционированного копирования //Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., № 5, 2002.* ***3.*** *Мюллер Скотт, Модернизация и ремонт ПК, 13-е издание.: Пер. с англ. – М.: Издательский дом «Вильямс», 2002. – 1184 с.*