

ЛІТЕРАТУРА

1. Берлянт А.М. Геообразження в Інтернеті // ГИС-обозрение. –1999. -№ 1. –С.11-15.
2. Кошкарєв А.В., Тикунов В.С., Лисицкий Д.В. Геоинформатика -М : Картогеоцентр Геоиздат, 1993 -213 с.
3. Архіпов О., Голованов Ю. Інтернет як основа для

- створення ГІС // ГИС-Обозрение – 1998. -№ 2. –С.19-21
- 4 Цветков В.Я. Основы ГИС – М.: Финансы и статистика, 1998. -281 с
5. PostgreSQL 7.3.1 Documentation // The PostgreSQL Global Development Group, 2002.

Надійшла до редколегії 03.07.2003

СТРУКОВ В.М., БАБИЙ А.С. К ПРОБЛЕМЕ ПРИМЕНЕНИЯ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ В СЕТЯХ ОВД

Предлагается новая технология реализации геоинформационных систем в сетях ОВД на основе оригинальных программных и web-технологических решений.

STRUKOV V.M., BABY A.S. TO THE PROBLEM OF APPLICATION OF GEOINFORMATION SYSTEMS IN NETWORKS OF LAW-ENFORCEMENT ORGANS

The new technology of realization of geoinformation systems in networks of law-enforcement organs is offered on the basis of original program and web-technological decisions.

УДК 004.056.53:004.085.2

В.В. ТОРЯНИК, канд. фіз.-мат. наук,
Г.Є. ГРИГОР'ЯНЦ, **М.В. ЦУРАНОВ**

Національний університет внутрішніх справ

СУЧАСНІ ПРИНЦИПИ Й МЕТОДИКИ ЗАХИСТУ КОМПАКТ-ДИСКІВ ВІД КОПІЮВАННЯ

Проведено аналіз існуючих систем захисту компакт-дисків від копіювання. Виявлені характерні ознаки типу захисту та відповідні методи його подолання. Обґрунтована економічна недоцільність створення копії диск-на-диск. Розроблена система захисту компакт-дисків від копіювання на жорсткий диск комп'ютера.

1. Призначення та склад систем захисту від копіювання.

У сучасному світі цифрових технологій випадки незаконного копіювання і використання даних та пов'язане з цим питання про захист інтелектуальної власності є дуже актуальним [1].

Зараз найзручнішим мобільним носієм цифрових даних є компакт-диск (CD), що зумовлено його ємністю - в 500 разів більшою за ємність звичайної дискети, компактністю - 8 см міні-диск втричі компактніший за дискету, надійністю - стійкістю до перепаду температур, магнітних полів, механічних навантажень, високою швидкістю запису та зчитування інформації. Але, як і будь-який технічний засіб, CD не є абсолютно надійним за певну ймовірність його розриву під дією інерційних сил у високошвидкісному приводі, механічних ушкоджень (поломки чи подряпини), що виникають при помилках CD-приводу та в процесі експлуатації диска [2]. З огляду на це доцільно зробити резервну копію оригінального компакт-диска, що в більшості випадків дозволяється в ліцензійних угодах (наприклад, корпорація Microsoft [3] дозволяє робити резервні копії

своїх продуктів)

Слід зауважити, що покупець фактично платить гроші не за дані, а за компакт-диск, як матеріальний носій, на якому вони записані. Тому систему "компакт-диск й дані" не слід розглядати окремо, а вважати цілісною. Якщо порушити цілісність цієї системи (незаконним копіюванням), то економічно страждають і виробник CD, і виробник програмного забезпечення (даних)

Тому в основному захист дисків від копіювання орієнтований на заборону створення точної копії оригінального CD на інший CD, і, рідше, від його копіювання на жорсткий диск комп'ютера

За визначенням захист від копіювання – це модифікація первісного програмного коду таким чином, що він стає залежним від деяких зовнішніх впливів, що виробляються охоронним модулем при виявленні ключа [3, 4].

Розглянемо, що являють собою згадані у визначенні поняття.

Залежність від зовнішнього впливу.

Первісна незахищена програма може бути змінена

таким чином, що вона більше не буде працювати без впливу охоронного модуля. Це може полягати просто в звертанні програми до охоронного модуля, але все-таки кращий спосіб зробити програму залежною від цього модуля - це зашифрувати її. Шифрування є повною зміною двійкового коду програми таким чином, щоб ця програма більше не запускалася.

Охоронний модуль.

Це програмний код, що відновлює розглянуту програму і надає можливість завантажити програму чи ініціалізує її яким-небудь іншим способом. Причому це повинно відбуватися тільки в присутності деякого авторизуючого ключа обставинці повної конфіденційності. Це необхідно для того, щоб ніхто не міг імітувати те, що робить цей модуль, і називається безпекою програмного коду. Крім того, сам охоронний модуль повинний бути добре захищений, звичайно, за допомогою шифрування.

Фізичний ключ.

Це деякий фізичний пристрій чи об'єкт, що повинний бути присутнім як підтвердження прав на використання захищеної програми. Ключ може реалізовуватись в багатьох формах: оригіналі компакт-диску, ключовій дискеті, спеціальному електронному модулі чи смарт-карті та ін.

2. Існуючі системи захисту компакт-дисків: ефективність та ознаки.

Практика показує, що не існує абсолютно надійно захищеного від копіювання CD. Нижче наведені найбільш розповсюджені методи захисту та можливі шляхи їх обходу.

Захист віртуальним збільшенням довжини декількох файлів на CD, щоб вони займали об'єм, більший за об'єм CD. Це досягається установкою набагато більшої, ніж у дійсності, довжини файлу в образі диска. Файл практично накладається на безліч інших файлів. Оскільки захищеної таким чином програмі відома реальна довжина файлу, вона буде працювати нормально. Можливий шлях подолання такого захисту полягає у створенні образу диска для подальшого запису його спеціальною програмою.

Як варіант попереднього захисту, можна зробити оригінальний CD з даними, що виходять за межі місткості 80-хвилинного CD. Для копіювання диска в цьому випадку знадобиться спеціальний 90-хвилинний диск, який може не розпізнаватися певними моделями CD-приводів.

Розробка нових систем захисту стимулюється розвитком ринку мультимедійних дисків. Саме виробники таких дисків створюють власні системи захисту дисків, зокрема, шляхом розробки оригінального програмного забезпечення для перегляду чи прослуховування мультимедіа файлів, які використовують деякі спеціальні записані на CD позначки. Так, авторами були досліджені дві комерційні системи захисту мультимедіа дисків.

Перша система розроблена європейським підрозділом фірми Sony (www.sony.com) та основана на запису помилкового сектора даних у таблицю розміщення символів (TOC). Через помилки CD-привід не може його коректно зчитати, і тому не розпізнає аудіо-треки. Аудіоцентри, для яких і призначений такий диск, навпаки - не розпізнають трек з даними і коректно зчитують аудіо-треки. Такий захист може бути подоланий виключенням (на фізичному або логічному рівні) помилкових секторів.

Друга система розроблена російською фірмою "Навігатор" (www.cdboom.com) і полягає у записі індексної та фізичної міток, які не дозволяють стандартно зчитати файли з диску, але розроблена фірмою оригінальна програма, що вміщена на диску, коректно їх обробляє. Можливий шлях подолання такого захисту - це зробити образ диска з метою подальшого його перепису на інший компакт-диск.

Виробники програмного забезпечення для персональних комп'ютерів використовують цілу низку різноманітних методів захисту. Аналіз найбільш застосованих методів та їх недосконалість з точки зору авторів подано нижче.

Диски, що мають нестандартні проміжки між аудіо треками й індексні відмітки в несподіваних місцях не копіюються більшістю програм, а на приводах, що не підтримують режим disc-at-once, може виявитися також неможливим скопіювати їх.

Нестандартні диски з треком коротше, ніж 4 секунди, створюють програмно-апаратні проблеми для більшості записуючих приводів. Захищений в такий спосіб додаток повинний перевіряти присутність і розмір такого треку. Деякі рекордери, однак, можуть справитись з такою задачею.

Це один метод полягає у розміщенні безлічі треків з даними, що перемежовуються аудіо-треками. Це порушує роботу деяких програм-дублюаторів дисків.

При звичайному файлового перезаписі диска можуть бути порушені службові мітки (мітка гучності, ім'я диску тощо), які є умовою коректної роботи захищених програм. Тому перевірка імені диска при копіюванні іноді корисна, але не дуже ефективна.

Окрім вказаних, існує безліч комерційних систем захисту CD, принцип роботи яких тримають у секреті. Однак, існують програми для злому практично кожної найбільш розповсюдженої системи захисту, а також програми для виявлення типу захисту CD [5]. Деякі типи захисту досить просто знайти за наступними ознаками, що полегшує подальший пошук метода знешкодження захисту.

CD Cops: при запуску основного файлу, що виконується, виникає вікно зі словами в заголовку "CD Cops", а в інсталяційній директорії присутні файл `cdscops.dll` і файли з розширеннями `gz` і `w_x`.

Disc Guard: на диску чи в інсталяційній директорії мають файли `ioslink.vxd` і `ioslink.sys`.

LaserLock: на диску мається схована директорія "Laserlock", що містить файли, при спробі копіювання яких з'являється повідомлення про помилку.

LockBlocks: захищений диск має 2 кола (шириною 5 і 3 мм).

Protect CD основний виконуваний файл містить повторюваний кілька разів ASCII текст "VOB" (шукати за допомогою HexEditor).

SafeDisc: на диску маються файли 00000001.tmp, clcd16.dll, clcd32.dll, clocspl.exe, dplayerx.dll.

SafeDisc 2: на диску присутні файли 00000001.tmp і 00000002.tmp

SecuROM: в інсталяційній директорії чи на диску маються файли cms16.dll, cms_95.dll, cms_nt.dll. Крім того, на упаковці чи на диску ви побачите напис "DADC", а при відкритті основного файлу, що виконується, Hexeditor'ом можна знайти ASCII текст "CMS".

Dummy Files/CD Lock: присутні великі dummy-файли (іноді їхній обсяг більше 600Mb) у кореневій директорії диска, звичайно з розширенням .afr

Illegal TOC: на CD маються 2 DATA-треки (звичайно розділені AUDIO-треком).

На нашу думку, при розробці систем захисту компакт-дисків бажано уникати ситуацій коли захист можна розпізнати шляхом пошуку на диску певних ознак (файлів чи директорій), а також фізичних особливостей (подряпини, специфічні окружності), бо це дозволяє не тільки легко розпізнати захист, але й цілеспрямовано шукати поради й програми для його знешкодження.

3. Економічний аналіз процесу копіювання компакт-диску.

Як показано в розділі 2, практично можливе створення точної копії будь-якого CD. Однак витрати (як інтелектуальні, так і економічні) на виготовлення точної копії диска не завжди себе виправдують.

Ми провели економічний аналіз типового процесу копіювання диск-па-диск і з'ясували, що орієнтовно вартість виготовлення точної копії диска в домашніх умовах складають¹:

- покупка сучасного записуючого приводу CD-RW (здатного читати канали субкодів) складе мінімально 320 грн.;

- диски для запису будуть коштувати від 2 до 10 грн., у залежності від місця покупки диска і характеристик диска;

- програмне забезпечення для злomu захисту вихідного диска і запису диска-копії може коштувати від 20 грн. (і значно більше у випадку придбання ліцензійних версій програм або з урахуванням витрат на пошук і завантаження таких програм з мережі Internet);

- витрати, пов'язані з візуальним оформленням диска-копії (спеціальна етикетка або маркер для нанесення записів) можуть скласти від 1 грн. і вище (друк етикетки, придбання та оформлення коробки).

З огляду на вищевикладене, можна зробити висновок, що перша копія ліцензійного диска може обійтися значно дорожче, ніж оригінальний диск. Окрім того, важливо, що диск, записаний самотужки, може не розпізнаватися на цілому ряді приводів CD-ROM. У випадку копіювання, наприклад, ліцензійних ігор вартістю від 15 грн., навіть і друга копія може виявитися невигідною.

Умовою зниження вартості диска-копії є повне відмовлення від візуального оформлення, упаковки і покупка більш дешевих дисків для запису, що спричинить суттєве зниження надійності збереження інформації. Якщо ж врахувати зусилля і час, витрачений на освоєння програм запису і злomu, а також час, витрачений безпосередньо на сам процес злomu і запису, то стає очевидним, що більшість користувачів відмовляться від створення точної копії оригінального диска на інший диск.

Таким чином, більш "доцільнішим", і в деяких випадках - ефективнішим способом незаконного використання програм та даних, є безпосереднє копіювання CD на жорсткий диск або використання програм віртуальних CD-ROM'ів, що емулюють привід CD-ROM попередньо скопіювавши дані з диска. Тому автори поставили за мету створення системи захисту саме від такого варіанту копіювання.

4. Технологія захисту DDD.

З огляду на результати економічного аналізу, авторами була розроблена власна технологія захисту CD, яка перешкоджає як копіювання на жорсткий диск комп'ютера, так і можливість зробити точну копію диска. У ході реалізації поставлених цілей опрацьована багатоступенева методика захисту диска, розроблений її алгоритм для програмної реалізації у виді двохмодульної програми DDD (Data Defense Disk).

Розроблена технологія містить у собі:

- аналіз фізичного носія даних,
- аналіз присутності на диску "ключа";
- аналіз дійсності "ключа";

- кодування первинних даних перед їхнім записом на фізичний носій.

Особливостями технології DDD є:

- аналіз фізичного носія за допомогою стандартних функцій операційної системи Windows, які дозволяють дістати дані про диск та привід (наприклад, дійсно це привід CD-ROM чи жорсткий диск комп'ютера) [6, 7],

- розроблений оригінальний метод аналізу носія (аналіз присутності "ключа" на диску та відповідності оригінальним секцій Lead in та Lead out [8])

Комбінація стандартного та оригінального методів аналізу дає можливість збільшити надійність секцій аналізу носія і зменшити ризик помилкової ідентифікації оригінального носія.

Наступним елементом захисту є шифрування даних (чи програмного коду) за допомогою власного алгоритму. Особливості алгоритму шифрування полягають у

¹ Аналіз приведено за цінами на 01.07.2003 р.

наступному:

- швидкість шифрування / дешифрування даних (у порівнянні з відомим алгоритмом шифрування MIME застосованому у Windows Commander швидкість більше у 4 рази), що не обмежує його використання для кодування великих за обсягом файлів даних, особливо на застарілих комп'ютерах [9];

- кодування великих файлів без значного збільшення їхньої довжини;

Програма реалізація алгоритму розбита на два окремих модуля: модуль шифрування і захисний модуль, сполучений з модулем дешифрування. Модуль шифрування недоступний кінцевому користувачу захищеного CD, а захисний модуль записується на оригінальний CD і виконує всі службові операції (аналіз носія, діалог з користувачем, дешифрування даних, надання користувачу оригінальних даних).

Таким чином нами створено програмний комплекс під назвою "DDD" Його функціональні особливості:

- малий розмір (700 kb);
- можливість захисту програмних файлів (exe, .com, .bat);
- можливість захисту файлів стандартних форматів (txt, doc, pdf, xls і in);
- можливість вибору виду захисту - або тільки захист від копіювання на жорсткий диск комп'ютера, або захист як від копіювання на інший CD, так і від копіювання на жорсткий диск;

- застосовність на "повільних" застарілих комп'ютерах

Програма пройшла первинне тестування на кафедрі захисту інформації та спеціальної техніки Національного університету внутрішніх справ, яке показало, що в цілому запропонований метод ефективно захищає CD від копіювання на жорсткий диск комп'ютера та від створення точної копії оригінального диску.

Висновки.

Більшість комерційних систем захисту CD не захищають диск від копіювання на жорсткий диск комп'ютера, та мають явні ознаки, які дозволяють полегшити розпізнання та знешкодження захисту. Згідно даним, отриманим у ході економічного аналізу процесу копіювання дисків встановлено, що в більшості випадків доцільніше зробити копію на жорсткий диск

комп'ютера. Цей факт варто ураховувати при розробці нових систем захисту. Автори також вважають, що при проектуванні системи захисту CD слід уникати ситуацій, коли тип захисту можливо розпізнати за певними програмними ознаками або фізичними особливостями носія. Також бажано розробляти універсальні й керувані системи захисту, що дозволяють захистити CD як від копіювання на інший CD, так і від копіювання на жорсткий диск комп'ютера з можливістю вибору окремої функції або їх комбінування. Запропонована авторами технологія позбавлена більшості недоліків сучасних систем захисту CD, спроектована з урахуванням вищевказаного та дозволяє захищати оригінальний диск від копіювання як на жорсткий диск комп'ютера так і на інший CD

ЛІТЕРАТУРА

1. Григор'янц Г.Є., Цуранов М.В. Принцип створення захищених даних на оптичних носіях // Актуальні проблеми сучасної науки і правоохоронної діяльності: Матеріали X наук.-практ. конф. курсантів та слухачів. –Харків: Нац. ун-т внутр. справ, 2003. –С.282-283.
2. Овсянников В. Тиражирование компакт-дисков - URL: <http://www.epos.kiev.ua/pubs/nk/tcd3.htm>
3. Базовые правила лицензирования. -URL: <http://www.microsoft.com/rus/licensing/general>.
4. Глушаков С. В. Создание и запись CD. Харьков Фолио, 2003. –391 с.
5. Диски, защищенные от записи – определяем наличие защиты. -URL: http://www.ntech.ru/cd/soft/protectiondetect_1.htm.
6. Павловская Т.А. С/С++. Программирование на языке высокого уровня. –СПб: Питер, 2003. –461 с.
7. Верма Р.Д. Справочник по функциям Win32 API. М.: Горячая линия - Телеком, 2002. –488 с.
8. Носов В.В., Манжай А.В. Защита данных на компакт-дисках от несанкционированного копирования. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. –2002. –№ 5.
9. Румянцев П.В. Работа с файлами в Win32 API. – М.: Горячая линия - Телеком, 2002. –246 с.

Надійшла до редакції 22.06.2003

ТОРЯНИК В.В., ГРИГОР'ЯНЦ Г.Є., ЦУРАНОВ М.В. СОВРЕМЕННЫЕ ПРИНЦИПЫ И МЕТОДИКИ ЗАЩИТЫ КОМПАКТ-ДИСКОВ ОТ КОПИРОВАНИЯ

Выполнен анализ существующих систем защиты компакт-дисков от копирования. Выявлены характерные признаки типа защиты и соответствующие методы ее преодоления. Обоснована экономическая нецелесообразность процесса копирования диск-на-диск. Разработана система защиты компакт-дисков от копирования на жесткий диск компьютера.

TORYANIK V.V., GRIGORIANZ G.E., ZURANOV M.V. THE MODERN PRINCIPLES AND METHODS FOR COMPACT DISCS COPY PROTECTION

The analysis of existing systems for copy protection was carried out. Typical signs of copy protection types and corresponding get over methods were revealed. Economical purposelessness of disk-to-disk copy was grounded. The system of protection from copying CD-to-HDD was worked out.