УДК 638.235.231 **Ткачов П.О., Сіницький О.М.**

РЕАЛЬНИЙ ЗАХИСТ ІНФОРМАЦІЇ НА ОПТИЧНИХ НОСІЯХ ВІД НЕЛЕГАЛЬНОГО КОПІЮВАННЯ. ЧАСТИНА ІІ

У першій части частині цієї статті було розглянуто загальний стан ситуації с піратством програмних засобів (ПЗ) у світі та в Україні. Були наведені основні рекомендації від Business Software Alliance (BSA) та IDC, які мають сприяти зменшенню рівня піратства. Рекомендації цих відомих та поважних організацій носять здебільше політичний, загальнодержавний характер [10] . Спробуємо розглянути технічні засоби, які можуть бути використані для забезпечення захисту інформації, яка розповсюджується на оптичних носіях від нелегального копіювання.

Технологія запису та використання інформації на компакт-дисках є, безсумнівно, одним із найвидатніших феноменів нашої ери. Починаючи з 1982 року, коли було прийнято перший формат для запису аудіо даних CD-DA, та цифрових даних CD-ROM у 1986 році, ця індустрія зробила низку великих кроків у майбутнє. Нові формати носіїв, такі як DVD та Blu-Ray Disc вже міцно ввійшли у наше життя. Синонімом поняття компакт-диску(CD) є оптичні носії та носії мультимедіа інформації.

Фізична структура усіх типів компакт-дисків представлена на рис.1. Товщина дисків складає 1,2 мм. Розміри не є точними і наведені для загального випадку.

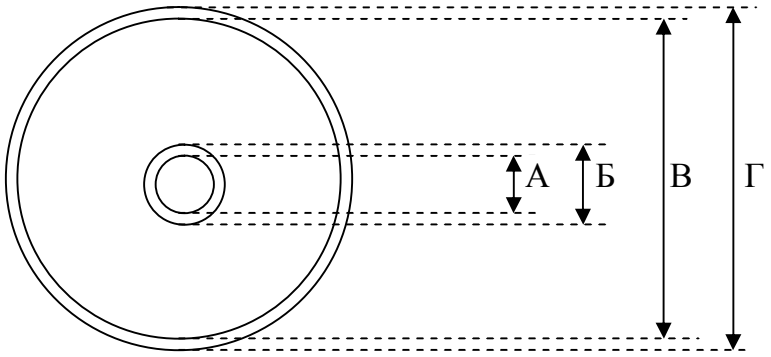

Рис. 1. Типовий мультимедіа диск

А - центральний отвір 15 мм

Б - початок спіральної доріжки від 44 до 50 мм

В - кінець спіральної доріжки від 76-77 до 116-117 мм

Г - зовнішній діаметр 80 або 120 мм

Дані записуються треками на внутрішньому шарі диска, який має певні відбиваючі властивості. Кількість треків залежить від типу диску. Шарів може бути один чи два. Запис виконується по спіралі. Напрямок запису першого шару відбувається від внутрішнього радіусу диску до зовнішнього. Другий шар може бути записаний як паралельно першому шарові (parallel track path – PTP), так і у протилежному напрямку від зовнішнього радіусу до внутрішнього (opposite track path – OTP). Зони для запису можуть бути на одній стороні диску чи на обох його сторонах. Такі диски називають двохсторонніми. Зона для запису має назву інформаційної зони (Information Zone). Кожна інформаційна зона розподіляється на три частини: внутрішня (Inner), зона даних (Data Zone) та зовнішня (Outer Zone) [9].

Внутрішня зона розділяє фізичний початок зони для запису або перезапису даних від початку зони даних. Зона даних зарезервована для запису даних користувача. Зовнішня зона розділяє зону даних від фізичного кінця зони запису/перезапису.

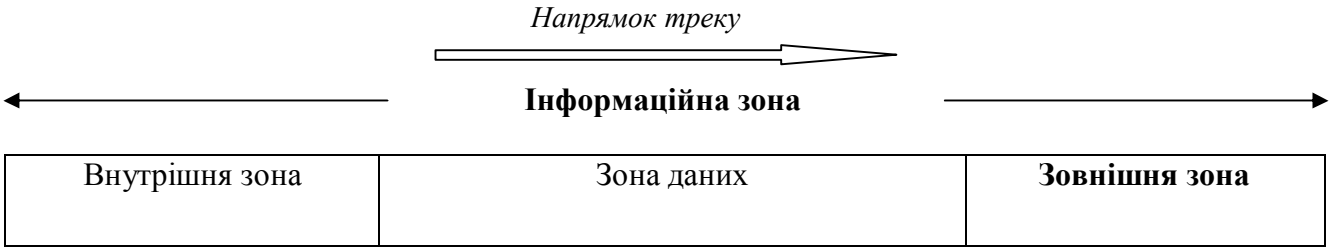

Рис. 2. Типова спіральна структура мультимедіа диску

Структура компакт-дисків для запису з одним шаром (Single Layer)

Розглянемо більш детальніше структуру компакт-дисків для запису з одним шаром. На таких одношарових дисках зона Lead-In являє безперервну зону, яка відноситься до внутрішньої зони та суміжну до зони даних. Для деяких форматів дисків ці зони збігаються. Зона Lead-In містить інформацію про формат, у якому може відбуватися запис таких дисків, а також детальну інформацію про фізичні характеристики диску. Зона Lead-Out відноситься до зовнішньої зони і містить додаткову інформацію про структуру записаного диску. Для деяких форматів запису така зона може також збігатися із зовнішньою зоною.

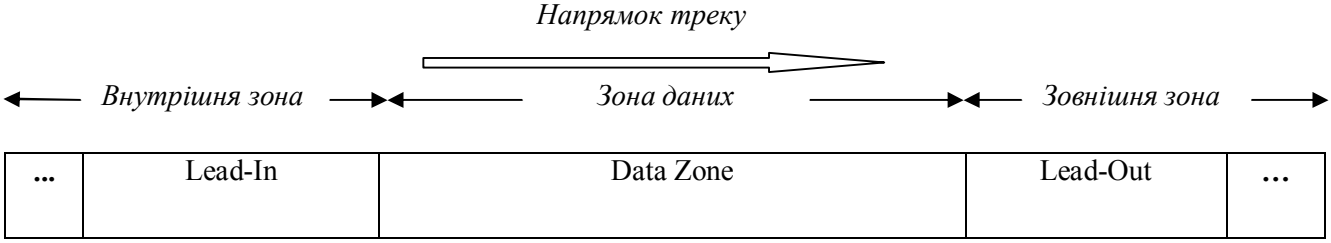

Рис. 3. Типова спіральна структура одношарового мультимедіа диску (Single Layer)

Структура компакт-дисків для запису з двома шарами (Dual Layer PTP)

Двошаровий диск з паралельним напрямком треків містить дві незалежні інформаційні зони, кожна я яких має структуру, аналогічно одношаровому диску. Кожен трек має власну зону Lead-In , Data Zone та Lead-Out, структура яких аналогічна структурі цих зон для одношарового диску.

Рис. 4. Типова спіральна структура одношарового мультимедіа диску (Dual Layer PTP)

Структура компакт-дисків для запису з двома шарами (Dual Layer OTP)

Двошаровий диск із зустрічним напрямком треків також містить дві незалежні інформаційні зони. Є додаткова зарезервована перехідна зона Middle Area. Структура інших зон аналогічна структурі зон для одношарового диску.

Рис. 5. Типова спіральна структура одношарового мультимедіа диску (Dual Layer OTP)

Логічна структура компакт-диску

Як вже було сказано вище, кожен шар диску може мати один чи більше треків, кількість яких залежить від типу компакт-диску. Нумерація треків та сесій завжди починається з 1. Декілька треків становлять таке поняття, як сесія. На рис. 6 зображена логічна структура диску, який має X-сесій, а друга сесія складається із K-треків.

Рис. 6. Типова логічна структура мультисесійного компакт-диску

Визначення файлової системі CDFS

Інформація на зовнішні носії записується структуровано. Така структура називається файловою системою. Файлова система забезпечує для програм стандартний спосіб доступу до даних. Наприклад, Windows використовує для доступу до даних, які записані на вінчестері, такі файлові системи як FAT32, NTFS. Доступ до даних, які записані на компакт-диску, забезпечується за допомогою файлової системи CDFS (стандарт ISO 9660). Для Unix-систем формат має назву Rock Ridge Interchange Protocol (RRIP) і був адаптований до вимог ISO 9960. Це гарантує сумісність CD-дисків для різних комп'ютерних систем типу Windows та Unix. Для комп'ютерів Macintosh використовується Hierarchial File System (HFS), яка не сумісна ні з Windows, ні з Unix. Стандарт ISO 9660 визначає ієрархічну файлову структуру у

протилежність до лінійної структури треків. Ієрархічна організація файлового каталогу дає можливість більш гнучкого доступу до файлів. У якості первинної точки входу визначена метка диску, яка має назву Primary Volume Descriptor (PVD) із фіксованим розміщенням на диску. PVD містить адресу розміщення кореневого каталогу та путь до таблиці, у який запам'ятовуються адреси усіх файлів [6].

Фізична структура компак-диску CD-DA та CD-ROM

Сімейство мультимедіа дисків типу CD можна розподілити на три основні групи:

- CD-DA
- CD-ROM
- CD-Recordable

Формат CD-DA (Compact Disc Digital Audio system) прийнятий у 1982 році. На базі цього стандарту для запису цифрової інформації довільного змісту був розроблений формат CD-ROM і прийнятий у 1984 році [6]. Потік даних розбивається на фізичні порції інформації, які мають назву малих фреймів (Small Frames). Сукупність усіх даних на диску становить послідовний потік малих фреймів. Кожен байт у малому фреймі закодовано з використанням розширення з 8 біт до 14 біт (Eight-to-Fourteen modulation). Для більшої стійкості коду та придушення низькочастотних шумів (<20 КГц) до кожної послідовності біт у групі додається ще 3 біта. Кожен малий фрейм складається із 588 EFM-біт. Фізична структура малого фрейму наведена у таблиці 1.

Таблиця 1. Фізична структура малого фрейму

1-й синхро-шаблон (24 + 3 bits)	1-й байт даних субканалу (14 + 3 bits)	12 байт основного каналу даних (12x(14+3) bits)	4 байта CIRC кода (4x(14+3) bits)	12 байт основного каналу даних (12x(14+3) bits)	4 байта CIRC кода (4x(14+3) bits)
588 біт					

Кожен CD-фрейм складається із 98 послідовних малий фреймів. Таким чином, один блок має 24*98 = 2352 байта основних даних на фрейм та 98 байт даних субканалу [6]. Записаний CD-диск є послідовність CD-фреймів. Для CD-DA дисків межі фреймів визначаються даними субканалу. Для CD-DATA дисків такі межі визначаються послідовністю біт синхронізації у основному каналі даних. 98 біт у субканалі розподілені на 2 біта синхронізації та 96 біт даних субканалу. Фізична структура диску CD-DA та CD-DATA наведена на рисунку 7.

Кількість байт у логічному блоці даних називають довжиною блоку. Кожен логічний блок має фіксовану для нього довжину. Для дисків у форматі CD-DA довжина логічного блоку становить 2352 байта та для CD-DATA 2048 байт. Загальна кількість логічних блоків становить 404850. Таким чином на CD-диск можна записати 404850*2048 = 829132800 байт або 790,7Мб. Але на практиці з метою сумісності з різними пристроями зчитування об'єм даних обмежують до рівня 700 Мбайт [6]. Для DVD-ROM,DVD-R та DVD-RW дисків з одним шаром кількість логічних блоків дорівнює 2295104. Максимальна місткість такого DVD-диску дорівнює 4,48 Гб. Для двохшарового DVD-диску кількість логічних блоків дорівнює 4173824, що становить загальну місткість у 8,1 Гб [7].

Технічні способи захисту компакт-дисків від копіювання

Розробкою систем захисту автори цієї статті почали займатися з 2000 року. У наших роботах [1,2] наведені три методи реалізації такого захисту, які відбивають нашу точку зору на проблему у той час.

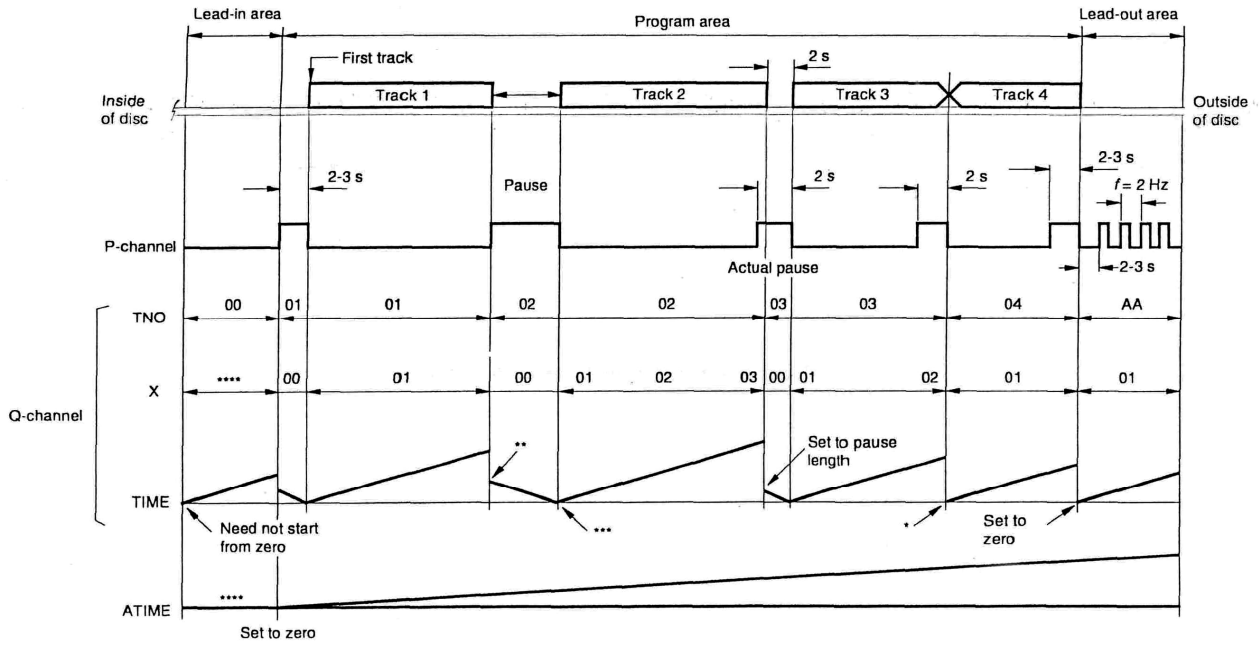

Рис.7. Фізична структура диску CD-DA та CD-DATA

Метод 1. Захист інформації шляхом внесення змін у деякі управляючі службові сигнали, які записані на диск синхронно з основним потоком даних.

Метод 2. Захист інформації шляхом запису на попередньо підготовлений носій, поверхня якого містить низку дефектів, які не можна усунути фізично, та які заважають перезапису диску, але не заважають його зчитуванню.

Метод 3. Захист інформації, який базується на внесенні змін до файлової системи.

Розглянемо більш детально вказані методи.

Метод 1. На компакт-диск синхронно з блоками даних формується і записується ряд керуючих цифрових сигналів. Подібний запис у переважній більшості випадків робиться апаратно й означає, що при цьому пристрій за допомогою внутрішнього генератора формує керуючі послідовності і розташовує їх наприкінці кожного блоку даних. Такі послідовності прийнято називати субканалами. Субканалів всього вісім і їх прийнято нумерувати рядковими англійськими буквами P,Q,R,S,T,U,V,W. Компакт-диски, записані в стандарті CD-DA та CD-DATA, використовують лише два субканали – P-субканал, що є стробовим при передачі даних від ініціатора до пристрою, і Q-субканал, в якому записується інформація про тайм-код, статус пристрою, коди апаратного коректора помилок, що працює за схемою Соломона-Ріда, а також деяка інша інформація.

Для подальшого використання було зарезервовано ще 6 субканалів – R-W, що на компакт-диск записуються, але фактично не використовуються. За період розвитку формату CD-DA в інші формати було зроблено лише кілька вдалих спроб використання R-W субканалів. Наприклад, у R-субканалі при записі диска у форматах CD-G і CD-TEXT записується деяка користувальницька інформація про копірайт та авторство для кожного треку. У рідких випадках інформацію з R-W субканалів використовують тестові програми для оцінки продуктивності того чи іншого пристрою читання/запису дисків. Практично, на сьогоднішній день ординарний компакт-диск, що містить інформацію довільного типу, несе в собі 75% незадіяних субканалів. Подібна ситуація дозволяє особливим чином захистити компакт-диск.

У процесі запису субканалів окремо від даних формуються цілком заповнені блоки, причому такий запис аж ніяк не порушує ніяких домовленостей і стандартів запису даних на

компакт-диск, але доповнює. В області невикористаних субканалів записується додаткова керуюча інформація, що неявно зв'язана з даними субканалів P і Q. Програма для запису захищених подібним чином дисків використовує дані Q-субканалу для формування W-субканалу. Дані, що будуть записані в W-субканал, є по суті закодовані симетричним алгоритмом відповідні керуючі дані. Первинний ключ для кодування формується на основі даних, записаних у службових областях на компакт-диску. Паралельно вводиться додатковий псевдостробуючий R-субканал.

Суть введення останнього полягає в тому, що частина записаних на диск даних розміщуються в область з вірним Q-субканалом, але з помилковим основним стробом. При читанні записаного в такий спосіб компакт-диску ці дані будуть просто ігноровані, не викликавши повідомлення про помилку. Однак, при використанні програми, здатної коректно читати подібні диски, перед прийняттям рішення про те, наскільки ефективна інформація, що читується, буде зроблена диз'юнкція реального і псевдостробуючого каналів, що забезпечить коректне і повне читання даних у всьому обсязі.

Зміст введення кодованого W-субканалу полягає в наступному. Більшість програм, які використовуються для копіювання компакт-дисків, не читають дані з області субканалів безпосередньо, але використовують вбудовані генератори або покладаються на можливості самого пристрою. При спробі перезапису диска з використанням подібних алгоритмів інформація із W і R субканалів буде загублена. Програма, яку було нелегально скопійовано, у процесі свого запуску або у процесі своєї інсталяції перевірить ультраструктуру субканалів носія, з якого зроблений запуск і в тому випадку, якщо декодування субканалу з програмно отриманим ключем не дасть контрольного результату, просто не буде працювати належним чином.

З поглядом на сьогоднішній час можна сказати, що даний метод автори цієї статті не змогли на 100 відсотків реалізувати за допомогою стандартних засобів, які надаються існуючими приладами для запису CD-R дисків. Іншими словами, за допомогою існуючих пишучих пристроїв зробити такі диски неможливо. Але ідея не втратила свого значення. Такий захист може бути реалізований тільки за умов використання спеціального обладнання, яке розташоване на заводах із виробництва компакт-дисків. Є цілком реальна технічна можливість модифікування стандартної технології виробництва, що може забезпечити реалізацію даного методу.

Метод 2. Дані повинні бути записані на диск, що містить "погані" для читання області. Подібні області не повинні заважати читанню даних жодним із прийнятих для даного формату методів. Спроби читання цих областей при копіюванні компакт-диску повинні закінчитися негативно і перервати процес копіювання. Існує цілий ряд пристроїв для запису компакт-дисків, що підтримують команди керування потужністю лазера і швидкістю обертання вала привода.

Необхідною і достатньою умовою наступного успішного читання даних, записаних подібним чином, є точний моніторинг збійних зон у момент запису. Це означає, що записуюча програма варіює параметри лазера до запису, після чого, при досягненні нормальних умов запису на поверхню диска в даному місці, записує ефективні дані. Причому дані Q-субканалу, які відповідають за позиціювання наступного не збійного сектора, формуються всередині пишучої програми, а не самим пристроєм і записуються окремо.

Таким чином, використовуючи цей алгоритм, ми можемо одержати захищений диск з практично будь-якими даними. Недолік цього методу складається у відчутному зменшенні загального обсягу даних, які можна записати при підвищенні ступеня захисту диска. Однак перевага методу в тому, що жодний пристрій та програма копіювання не зможе зробити точну копію такого диска. Звичайно користувач може нелегально скопіювати дані без дублювання структури диска, але легко реалізована програмна перевірка носія, з якого

запущена програма, не дасть можливості для запуску програми не з оригінального компакт-диску.

Даний метод був частково реалізований. Була проведена доробка на апаратному рівні пишучого CD-RW пристрою, внаслідок чого була отримана можливість на програмному рівні за допомогою стандартних команд запису компакт-дисків [8,9] керувати процесом створення "поганих" зон на диску під час його запису. Створені таким чином диски не копіювалися, але суттєвими недоліками виявились два моменти. По-перше, для таких дисків був виявлений дуже низький рівень сумісності з існуючими оптичними приводами. Іншими словами, такі диски могли бути прочитаними лише на окремих пристроях, а більшість інших пристроїв такі диски відмовлялася читати. І, по-друге, випуск таких дисків дуже важко або взагалі неможливо налагодити у заводських умовах.

Метод 3. Запис даних на будь-який носій завжди робиться структуровано. Метод побудови базових структур для упорядкування інформації на носіях прийнято називати файловою системою. Цей метод визначає такі параметри, як розмір апертури читання/запису (що іноді помилково називають довжиною сектора), спосіб формування директоріальних записів і таблиці розміщення, синхронізаційні дані і коди контрольних сум. Запис даних на компакт-диск здійснюється з використанням файлової системи CDFS. При цьому в службовій області формується таблиця розміщення даних, що містить вектори початку даних (чи доріжок файлів) і довжини.

Суть даного методу захисту полягає у використання нестандартної файлової системи при абсолютно стандартному записі таблиці розміщення. При записі сукупності даних на диск пишуча програма формує таблицю і записує її у відповідну частину службової області. При цьому запис про розмір даних залишається рівним нулю, а перший вектор даний вказує на область, у якій у стандартному CDFS-форматі записаний блок даних, що відповідають специфічній програмі-завантажнику. Власне дані пишуться після цього блоку вже у форматі захищеної файлової системи.

При спробі копіювання такого диску стандартна програма зчитування визначить, що диск заповнений, але сумарна довжина усіх файлів близька до нуля, і не зможе виконати копіювання. З іншого боку, при запуску з такого диска захищена програма вірно прочитає дані з областей з нестандартною файловою системою, після чого коректно почне працювати.

Даний метод був повністю реалізований і всебічно перевірений. В результаті від нього довелось відмовитися, тому що ряд популярних програм для копіювання, які з'явилися пізніше, успішно копіює таки диски. І знову ж таки суттєвим недоліком виявилась проблема сумісності з існуючими оптичними приводами та програмними засобами Windows.

Новий підхід до реалізації захисту. Технологія IronDisc

Як було сказано вище, спочатку компакт-диски були призначені тільки для запису музики і тільки через певний проміжок часу були адаптовані для запису цифрового контенту довільної форми. У таблиці 2 наведено фізичну структуру компакт-диску типу CD-DA та CD-DATA. Запис музики здійснюється двоканальним методом по 16 біт на канал з частотою 44,1 Кгц. Таким чином швидкість цифрового потоку при зчитуванні дорівнює 4x44100 = 176400 байт/сек. Довжина фізичного блоку даних або фрейму для формату CD-DA є 2352 байта. Якщо розділити 176400 на 2352, то отримуємо швидкість потоку даних 75 фреймів/сек. Адресація усіх фреймів на диску здійснюється у форматі MM:SS:FF або MSF, де MM - хвилини (0-99), SS – секунди (0-59), FF – фрейми (0-74) . Адреса першого фрейму для інформаційної зони є 00/00/00. Зони Lead-In та Lead-Out (див. рис. 1) теж мають свої визначені адреси у термінах MSF. Наприклад, останній фрейм у зоні Lead-In має адресу 99:59:74. Паралельно з адресацією у термінах MSF існує і "нормальна" адресація, де перший фрейм інформаційної області дорівнює 0, наступний 1 і так далі до 404849 номеру. Слід сказати, що між системами адресації існує взаємооднозначна залежність. Розмір

інформаційної зони був обраний у 90 хвилин. Перший фрейм дорівнює 00/00/00, а останній 89/59/74. Або від –150 до 404849. Зона Lead-In знаходиться у межах 90/00/00 – 99/59/74, або від –45150 до –151.

Для того, щоб не можна було зробити точну копію компакт-диску, необхідною і достатньою умовою є умова, щоб копія хоч би на один біт відрізнялася від оригінала, та існував алгоритм, який міг би виявити таку різницю. Чисельні експерименти виявили, що для розташування інформації в інформаційній зоні використовується адресна зона, яка починається не з 00/00/00, а із 00/02/00 (це фрейм з адресою 0).Таким чином, виявилось, що інформаційна зона з адресами фреймів від –150 до –1 (зона pre-gap) практично не використовується. На CD-DA ця зона містить двохсекундну паузу перед початком першого музичного треку, а для CD-DATA функціональність цієї зони не визначена. На базі цього факту і була розроблена система захисту комакт-дисків типу CD-DATA від несанкціонованого копіювання. USER DATA означає інформаційний блок, який записується на компакт-диск у адресному просторі від –4510 до –1. На рис. 8 наведено схематичне розташування інформації на захищеному компакт-диску.

Чисельні експерименти підтвердили той факт, що цю зону не копіює жодна програма – копіювальник. Це означає, що на копії, зробленої з захищеного диску, буде відсутня саме зона USER DATA (рис. 8). З іншого боку є можливість запису USER DATA в означену вище область за допомогою звичайних пишучих пристроїв на стандартних програмних засобів. Запис додаткової інформації у цю зону не порушує існуючих стандартів для такого типу дисків, внаслідок чого була вирішена і проблема сумісності. Захищені диски читаються усіма видами існуючих оптичних пристроїв типу CD/DVD. На цю ідею були отримані авторські свідоцтва України та Росії, а також патент США [3,4,5]. Був розроблений програмний комплекс, який має назву Guardian (2002 рік) та IronDisc (2008 рік), можливості якого дозволяють створювати захищені компакт-диски типу CD-R для невеликих тиражів (100-1000 шт.) за допомогою роботизованого коплексу на базі звичайного ПК та для дисків CD-ROM у заводських умовах будь яким тиражем.

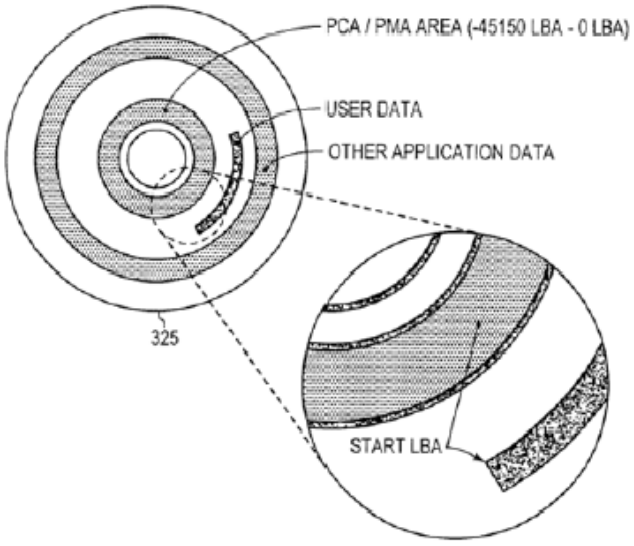

Рис. 8. Схема розміщення інформації на захищеному диску

На рис. 9 наведено алгоритм, за яким програма IronDisc розпізнає оригінальний компакт-диск або ж його копію.

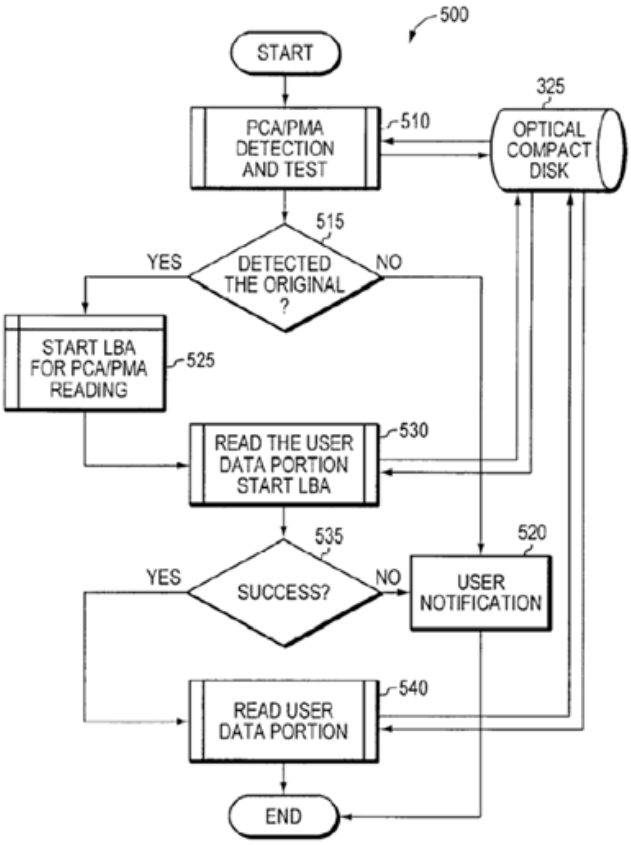

Рис. 9. Алгоритм розпізнавання для захищеного диску.

Більш детальна інформація наведена на сайті http://www.uvarta.com.

Список літератури

1. *Ткачев П.А., Синицкий А.Н., и др.* Защита информации на компакт-дисках от нелегального копирования и тиражирования. Безопасность информации. № 4(14). 2000.

2. *Ткачев П.А., Синицкий А.Н. и др.* Использование программно-аппаратных средств для защиты информации на компакт-диске от нелегального копирования и тиражирования. Третя науково-технічна конференція. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Тези доповідей. Жовтень 2001.

3. *Ткачов П.О., Сіницкий О.М. та інші.* Комп'ютерна програма "Guardian". Свідоцтво про державну реєстрацію прав автора на твір. ПА № 4500. Україна. Липень 2001.

4. *Ткачев П.А., Синицкий А.Н.* Программа для защиты компакт-дисков от несанкциониро-ванного копирования и тиражирования "Guardian". Свидетельство об официальной регистрации программы для ЭВМ. №2002610215. Российская Федерация. Февраль 2002.

5. *Pavel Tkachev, Alexander Sinitsky.* Patent application. Storage medium. Attorney Docket No 025864-000300US. October 2008.

6. *Optical Disc Manufacturing Equipment.* The CD Family. Royal Philips Electronics. 1996.

7. DVD+R 4.7 Gbytes. Basic Format Specification. Royal Philips Electronics. July 2004.

8. *American National Standards Institute*. International Committee on Interface Technology Standards T10. Project 333-2000. May 2000.

9. *American National Standards Institute.* International Committee on Interface Technology Standards T10. Project 1836D. Revision 2a. November 2008.

10. Fifth Annual BSA and IDC Global Software. Piracy Study. 2008.

Надійшла 2.11.09