



ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

УКРАЇНА

(19) **UA**

(11) **100204**

(13) **U**

(51) МПК

G06F 12/14 (2006.01)

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2015 01620**

(22) Дата подання заявки: **24.02.2015**

(24) Дата, з якої є чинними
права на корисну
модель: **10.07.2015**

(46) Публікація відомостей
про видачу патенту: **10.07.2015, Бюл.№ 13**

(72) Винахідник(и):

**Розорінов Георгій Миколайович (UA),
Брягін Олег Володимирович (UA)**

(73) Власник(и):

**Розорінов Георгій Миколайович,
вул. Пироговського, 3, кв. 12, м. Київ, 03110 (UA),
Брягін Олег Володимирович,
вул. Маршала Рибалка, 3, кв. 8, м. Київ,
04116 (UA)**

(54) СПОСІБ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ВИКОРИСТАННЯ

(57) Реферат:

Спосіб захисту інформації від несанкціонованого використання стандартними програмно-апаратними засобами комп'ютера за допомогою ідентифікуючих технічних ключів. Як ключ використовують координати дефектних блоків флеш-накопичувача, який використовують одночасно з носієм інформації і за допомогою якого виконують ідентифікацію ключа.

UA 100204 U

Корисна модель належить до галузі обчислювальної техніки, зокрема до програмно-інформаційного забезпечення, і призначено для захисту інформації від несанкціонованого використання.

Відомий спосіб захисту інформації від несанкціонованого використання за допомогою ключів (пат. України № 55469 по кл. G06F12/14, за 2003 р.).

Як ключі можуть бути використані кодові карти: картонні, магнітні, оптичні. Найчастіше використовуються електронні ключі. Інформація, що захищається, в процесі роботи ідентифікує ключ, тобто запрошує код ключа і порівнює його з кодом, записаним в програмі. За наслідками ідентифікації інформація забезпечує реалізацію заданого регламенту її використання.

Недоліком цього способу захисту інформації є необхідність установки додаткового пристрою (ключа), унікального за записаним в ньому кодом.

Іншим відомим способом захисту інформації від несанкціонованого використання є захист паролем. Ключем в цьому випадку є користувач. Пароль, що вводиться користувачем на запит інформаційної програми є умовою для реалізації заданого регламенту використання інформації. Такий спосіб захисту інформації достатньо ефективний при обмеженому колі користувачів і їх зацікавленості в захисті інформації.

Недоліком цього способу є те, що він не може використовуватися у разі, коли потрібний захист інформації масового використання, оскільки повідомлення пароля великій кількості користувачів, зазвичай не зацікавлених в захисті інформації, швидко призводить до падіння ефективності захисту.

Відомий спосіб захисту інформації, що полягає в тому, що на носіїв інформації (наприклад, диску) механічним, магнітним, оптичним або іншим способом наносяться у випадковому порядку дефекти на записуюче покриття (патент РФ № 2109331, кл. G06F12/14 за 1998 р.). Під дефектом розуміється така зміна покриття, на місці якої неможливий запис інформації, але це не перешкоджає використанню носія за прямим призначенням. Згідно з цим способом виконується 2-3 зміни, кожна з яких захоплює 2-3 сектори. Далі носій розмічається стандартним чином, і при цьому визначаються координати дефектних секторів (номери секторів або інші прийняті координати для носіїв інформації). Ці координати в неявному (замаскованому) вигляді заносяться в записувану на носій інформацію.

Цей спосіб вибраний як найближчий аналог, оскільки він має ознаки, загальні із способом, що заявляється, а саме, наявні дефекти на записуючому покритті носія використовуються у вигляді елементів ключа.

Недоліком найближчого аналога є наявність ідентифікуючого ключа захисту, як такий використовується той же самий носій інформації.

В цьому випадку носій інформації, що захищається (ліцензійний), може бути використаний тільки на тому комп'ютері, на якому встановлена програма з ідентифікуючим ключем захисту. На інших комп'ютерах таку програму необхідно спеціально встановлювати, що створює певні незручності.

Крім цього, використання для копіювання носія інформації деяких програмних утиліт, які виконують клонування на фізичному рівні, наприклад "CloneCD", або "BlindRead" (див. Асмаков С. Диски под замком // Компьютер Пресс, № 3, 2002 р.) дозволяє відображати у клонованій копії також інформацію про ключі захисту, що значно знижує ефективність такої системи захисту.

В основу корисної моделі, що заявляється, поставлено задачу у відомому способі захисту інформації від несанкціонованого використання забезпечити можливість зчитування ліцензійної інформації на будь-якому комп'ютері без попереднього встановлення на них програм з ідентифікуючими ключами.

Такий спосіб захисту інформації особливо ефективний в умовах дії регламентів, які припускають передачу (пересилку) носіїв, на яких записана інформація з обмеженим доступом, наприклад інформація, віднесена до конфіденційної, або інформація, що отримується при реалізації норм кримінального процесуального права, обмеження доступу до якої необхідне для забезпечення таємниці слідства. Назвемо такий носій ліцензійним.

Поставлена задача вирішується за рахунок того, що в способі захисту інформації від несанкціонованого використання стандартними програмно-апаратними засобами комп'ютера за допомогою ідентифікуючих технічних ключів, як ключ використовують координати дефектних блоків флеш-накопичувача, який використовують одночасно з носієм інформації і за допомогою якого виконують ідентифікацію ключа.

Встановлення в один із роз'ємів портів введення-виводу флеш-накопичувача, із сформованими на ньому ідентифікуючими ключами, забезпечує додатковий захист від несанкціонованого використання інформації, що знаходиться на ліцензійному носіїв.

Суть корисної моделі полягає в наступному. Флеш-накопичувачі завжди мають дефектні блоки пам'яті, які утворюються на стадії їх виготовлення, а кількість таких дефектних блоків складає не більше 2 відсотків від загальної їх кількості (див. Marcel B., Martiende J., Coert K., Ronaldvander K., Mark R., Forensic Data Recovery from Flash Memory. Small Scale Digital Device Forensics Journal, Vol. 1, No. 1, June 2007, p. 1-17, на стор.2, або TN-29-59: "Bad Block Management in NAND Flash Memory", Micron Technology, Inc., на стор. 3).

Інформація щодо місця знаходження кожного дефектного блока фіксується у спеціальному програмному забезпеченні трансформації логічних даних у фізичні адреси флеш-накопичувача (Flash Translation Layer-FTL), а алгоритми поводження з дефектними блоками (Bad block Management, Invalid Block Management) є складовою частиною зазначеного спеціального програмного забезпечення (див. TN-29-59: "Bad Block Management in NAND Flash Memory", Micron Technology, Inc., на стор. 3).

Алгоритми поводження з дефектними блоками є такими, що унеможливають їх використання для запису інформації на флеш-накопичувач. Підключення флеш-накопичувача до операційної системи персонального комп'ютера відбувається за результатами виконання логічних операцій між цією системою та програмою FTL. Враховуючи те, що розподіл дефектних блоків, які утворюються під час виготовлення флеш-накопичувачів, має очевидну випадкову природу, а загальна їх кількість може складати від 82 для ємкості накопичувача у 4 Гбайти (загальна кількість блоків - 4 096) до 327 для ємкості накопичувача у 16 Гбайтів (загальна кількість блоків - 16 384) (див. Data Sheet of NAND Flash Memory MT29F4G08AAA, MT29F8G08BAA, MT29F8G08DAA, MT29F16G08FAA, Micron Technology, Inc., електронний ресурс: 09005aef81b80eac4gb_nand_m40a_1.fm-Rev. B 2/07 EN), тому можна використати наявну у FTL флеш-накопичувача інформацію про місцезнаходження дефектних блоків пам'яті, для формування ключа доступу.

Для створення ключа достатньо вибрати дані про місцезнаходження 3-х або більше дефектних блоків.

Визначити необхідні характеристики дефектних блоків можливо за допомогою одного з видів програмного забезпечення, яке застосовується для програмування флеш-накопичувача на низькому рівні. Ці характеристики (наприклад координати дефектних блоків) в неявному (замаскованому) вигляді заносяться в записувану на флеш-накопичувач програму і є ідентифікуючими ключами.

Користувач встановлює ліцензійний носій і одночасно запускає програму ідентифікації, що зберігається на флеш-накопичувачі. При цьому виконується процедура автентифікації сформованих на флеш-накопичувачі ідентифікаторів. За наслідками ідентифікації реалізується заданий на носіїв інформації регламент її використання, тобто програма може виконуватися або не виконуватися, переписуватися на інший носій тощо.

Захищеність інформації від несанкціонованого використання визначається відсутністю видимих координат на носіїв, робить дуже складним точне повторення дефектів, маскування координат ідентифікаторів і наявність ідентифікуючого флеш-накопичувача досить надійно захищає від спроб руйнування системи захисту, користувач усунений від організації захисту інформації.

Важливим є те, що захист здійснюється за допомогою стандартних програмно-апаратних засобів комп'ютера, що спрощує як організацію захисту, так і роботу користувачів із захищеною інформацією.

Пропонований спосіб захисту інформації особливо ефективний в умовах дії регламентів, які припускають передачу (пересилку) носіїв, на яких записана інформація з обмеженим доступом, наприклад інформація, віднесена до конфіденційної, або інформація, що отримується при реалізації норм кримінального процесуального права, обмеження доступу до якої необхідне для забезпечення таємниці слідства.

Реалізація корисної моделі не є складною. Методи визначення координат дефектних блоків флеш-накопичувача, хоча і не є простими, оскільки вимагають використання програмно-апаратних засобів (але це забезпечує додатковий захист від відтворення ідентифікаторів), але цілком здійсними, більш того, є стандартними операціями для програмно-апаратних засобів комп'ютера.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб захисту інформації від несанкціонованого використання стандартними програмно-апаратними засобами комп'ютера за допомогою ідентифікуючих технічних ключів, який **відрізняється** тим, що як ключ використовують координати дефектних блоків флеш-

накопичувача, який використовують одночасно з носієм інформації і за допомогою якого виконують ідентифікацію ключа.

Комп'ютерна верстка В. Мацело

Державна служба інтелектуальної власності України, вул. Василя Липківського, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601