УКРАЇНА

(19) UA (11) 91403 (13) U

(51) МПК (2014.01)
G06F 9/445 (2006.01)
G09C 1/00

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2013 09948**

(22) Дата подання заявки: **09.08.2013**

(24) Дата, з якої є чинними права на корисну модель: **10.07.2014**

(46) Публікація відомостей про видачу патенту: **10.07.2014, Бюл.№ 13**

(72) Винахідник(и):
Дмитришин Олександр Васильович (UA),
Каплун Валентина Аполінаріївна (UA)

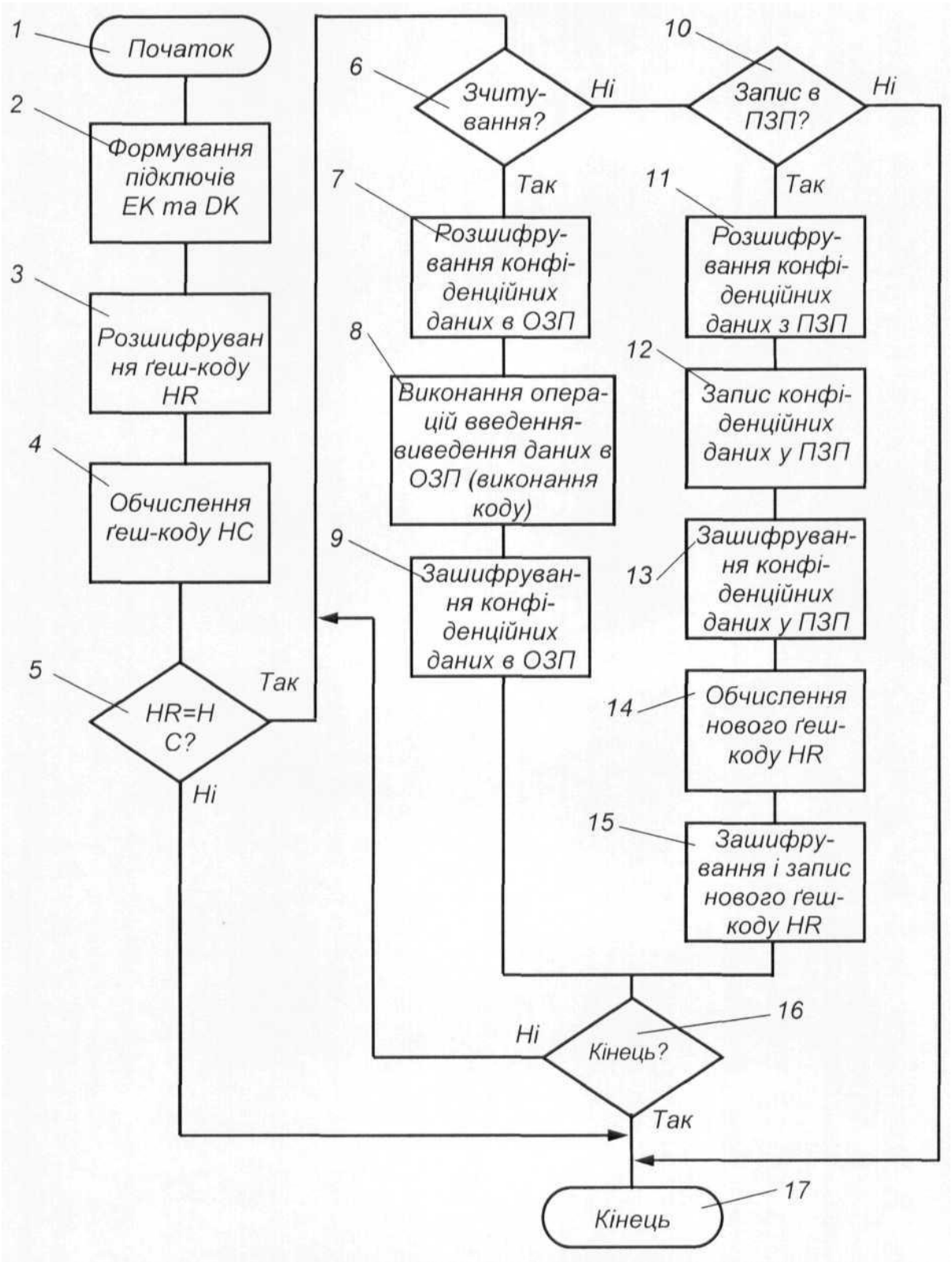
(73) Власник(и):
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ,
Хмельницьке шосе, 95, м. Вінниця, 21021 (UA)

(54) СПОСІБ КРИПТОГРАФІЧНОГО ЗАХИСТУ ВИКОНУВАНОГО ФАЙЛУ

(57) Реферат:

Спосіб криптографічного захисту виконуваного файлу полягає в тому, що вихідний файл доступний користувачу лише в захищеному вигляді. Розшифрування файлу виконується лише за наявності секретного ключа, зміни, які вносять в розшифрований файл, зберігаються в зашифрованому вигляді. Зашифруванню підлягають лише конфіденційні дані виконуваного файлу. Для захищеного файлу обчислюється хеш-код, який зашифровується та зберігається у тому ж самому захищеному файлі.

UA 91403 U


1
Початок
2
Формування підключів EK та DK
3
Розшифрування ґеш-коду HR
4
Обчислення ґеш-коду HC
5
HR=HC?
Так
Ні
6
Зчитування?
Ні
Так
7
Розшифрування конфіденційних даних в ОЗП
8
Виконання операцій введення-виведення даних в ОЗП (виконання коду)
9
Зашифрування конфіденційних даних в ОЗП
10
Запис в ПЗП?
Ні
Так
11
Розшифрування конфіденційних даних з ПЗП
12
Запис конфіденційних даних у ПЗП
13
Зашифрування конфіденційних даних у ПЗП
14
Обчислення нового ґеш-коду HR
15
Зашифрування і запис нового ґеш-коду HR
16
Кінець?
Ні
Так
17
Кінець

Корисна модель належить до галузі криптографічного захисту інформації і може бути використана для забезпечення захисту програмного забезпечення комп'ютерних систем від несанкціонованого використання.

Відомий спосіб захищеної обробки, який полягає в тому, що для файлу обчислюється цифровий підпис, який зберігається у тому ж самому файлі, далі виконується шифрування файлу, включаючи цифровий підпис, виконання операцій введення-виведення над файлом здійснюється без необхідності розшифрування всього файлу (Патент США № 0088783 A1, МПК H04L 9/00, 08.05.2003 р.).

Недоліками аналогу є те, що кожного разу при зверненні до відповідної частини виконуваного файлу, який на момент виконання зберігається в оперативній пам'яті комп'ютерної системи в зашифрованому вигляді, спочатку виконується операція розшифрування, а потім знову зашифрування, що зменшує швидкодію обробки даних.

Найбільш близьким за сукупністю ознак до запропонованого є спосіб захисту виконуваного файлу від несанкціонованого копіювання, який полягає в тому, що вихідний файл зашифровується і доступний користувачу лише в захищеному вигляді, розшифрування файлу виконується лише за наявності ліцензії користувача (в подальшому - секретний ключ), зміни, які вносять в розшифрований файл зберігаються в зашифрованому вигляді (Патент СІНА № 0078669 A1, МПК G06F 9/45, H04L 9/32, 31.03.2011 р.).

Недоліками способу-прототипу є недостатній рівень захищеності виконуваного файлу від несанкціонованого копіювання, оскільки після розшифрування файл розміщується в оперативній пам'яті комп'ютерної системи в незахищеному вигляді.

В основу корисної моделі поставлена задача створення способу криптографічного захисту виконуваного файлу, в якому за рахунок шифрування лише конфіденційних даних і обчислення хеш-коду для незахищених та зашифрованих даних виконуваного файлу досягається можливість підвищення швидкості обробки даних.

Поставлена задача вирішується тим, що в спосіб криптографічного захисту виконуваного файлу, який полягає в тому, що вихідний файл доступний користувачу лише в захищеному вигляді, розшифрування файлу виконується лише за наявності секретного ключа, зміни, які вносять в розшифрований файл, зберігаються в зашифрованому вигляді, зашифруванню підлягають лише конфіденційні дані виконуваного файлу, для захищеного файлу обчислюється хеш-код, який зашифровується та зберігається у тому ж самому захищеному файлі.

На кресленні зображена схема роботи програми, що захищає виконуваний файл, яка містить процедуру запуску файлу на виконання 1, процедуру формування підключів зашифрування EK та розшифрування DK 2, процедуру розшифрування хеш-коду HR 3, процедуру обчислення хеш-коду HC 4, умовний оператор перевірки цілісності виконуваного файлу 5, умовний оператор зчитування/запис даних в оперативно запам'ятовуючий пристрій (ОЗП) 6, процедуру розшифрування конфіденційних даних в ОЗП 7, процедуру виконання операцій введення-виведення даних в ОЗП (виконання коду) 8, процедуру зашифрування конфіденційних даних в ОЗП 9, умовний оператор запису даних у виконуваний файл, що зберігається в постійно запам'ятовуючому пристрої (ПЗП) 10, процедуру розшифрування конфіденційних даних з ПЗП 11, процедуру запису конфіденційних даних у ПЗП 12, процедуру зашифрування конфіденційних даних у ПЗП 13, процедуру обчислення хеш-коду HR 14, процедуру зашифрування і запису нового хеш-коду HR 15, умовний оператор завершення роботи виконуваного файлу 16, процедуру завершення виконання файлу 17.

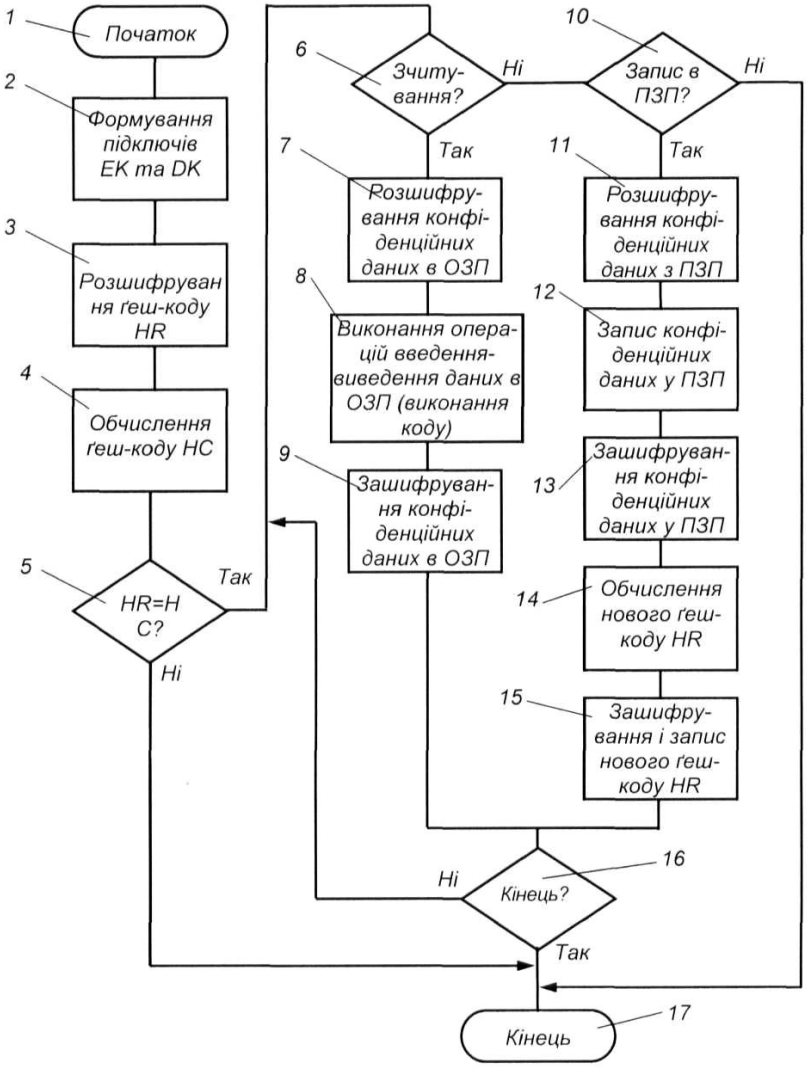
Спосіб криптографічного захисту виконуваного файлу здійснюють таким чином.

На етапі проектування програмного засобу у виконуваному файлі визначаються частину коду, що містять конфіденційні дані, які зашифровуються за допомогою симетричного блокового шифру на секретному ключі K. За допомогою хеш-функції для захищеного файлу обчислюється хеш-код, який зашифровується та дописується до виконуваного файлу. В подальшому після запуску програми на виконання 1 з секретного ключа K виконується розширення ключів зашифрування EK та розшифрування DK 2, розшифровується хеш-код HR 3, що зберігається у виконуваному файлі та обчислюється хеш-код для захищеного виконуваного файлу HC 4. Отримані значення порівнюються 5, якщо HR≠HC, то цілісність виконуваного файлу була порушена та виконується завершення роботи, в протилежному випадку продовжується виконання файлу. Якщо виконується звернення до конфіденційних даних, які розташовані в ОЗП 6, то такі дані розшифровуються 7, далі залежно від виду конфіденційних даних виконується операція введення-виведення даних в ОЗП або виконання конфіденційного коду файлу 8, після чого конфіденційні дані зашифровуються 9. Якщо виконується запис конфіденційних даних у виконуваний файл, що розташований в ПЗП 10, то відповідна частина файлу розшифровується 11, далі виконується запис конфіденційних даних у ПЗП 12 та

зашифрування розшифрованих та оновлених даних 13, обчислення нового хеш-коду HR 14, його зашифрування та запис у виконуваний файл, що знаходиться в ПЗП 15. Якщо виконується умовний оператор 16, то виконується завершення роботи програмного засобу 17, в протилежному випадку виконання програми продовжується з аналізу керуючих даних, що надходять на вхід умовного оператора 6.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб криптографічного захисту виконуваного файлу, який полягає в тому, що вихідний файл доступний користувачу лише в захищеному вигляді, розшифрування файлу виконується лише за наявності секретного ключа, зміни, які вносять в розшифрований файл, зберігаються в зашифрованому вигляді, який **відрізняється** тим, що зашифруванню підлягають лише конфіденційні дані виконуваного файлу, для захищеного файлу обчислюється хеш-код, який зашифровується та зберігається у тому ж самому захищеному файлі.



Комп'ютерна верстка М. Мацело

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

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