



УКРАЇНА

(19) UA (11) 66790 (13) U
(51) МПК
H04L 9/14 (2006.01)

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під
відповідальність
власника
патенту

(54) СПОСІБ ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ У КРИПТОГРАФІЧНИХ ЗАСОБАХ ЗАХИСТУ ІНФОРМАЦІЇ

1

2

(21) u201113881

(22) 25.11.2011

(24) 10.01.2012

(46) 10.01.2012, Бюл.№ 1, 2012 р.

(72) МАРТИНЕНКО СЕРГІЙ ВАСИЛЬОВИЧ, БЕЛОВ СЕРГІЙ ВАЛЕНТИНОВИЧ, РОМІН ОЛЕКСАНДР ОЛЕКСІЙОВИЧ, КРАВЦОВ ГРИГОРІЙ ОЛЕКСІЙОВИЧ, ЗУБАРЕВА ОЛЕНА ОЛЕКСАНДРІВНА

(73) МАРТИНЕНКО СЕРГІЙ ВАСИЛЬОВИЧ, БЕЛОВ СЕРГІЙ ВАЛЕНТИНОВИЧ, РОМІН ОЛЕКСАНДР ОЛЕКСІЙОВИЧ, КРАВЦОВ ГРИГОРІЙ ОЛЕКСІЙОВИЧ, ЗУБАРЕВА ОЛЕНА ОЛЕКСАНДРІВНА

(57) 1. Спосіб застосування криптографічних алгоритмів у засобах захисту інформації, який полягає у тому, що застосовують криптографічні алгоритми, вбудовані виробником на стадії виробництва або підготовки його до експлуатації, для реалізації криптографічних функцій, який **відрізняється** тим, що складається з наступних етапів:

-записують спеціальне програмне забезпечення (СПЗ), у якому реалізують обробку запитів від внутрішніх програмних застосувань на виконання криптографічних перетворень у відповідності до алгоритмів, закладених виробником пристроїв або створених за правилами, передбаченими виробником для інших криптографічних алгоритмів;

-у засіб криптографічного захисту інформації (КЗІ) записують спеціальне програмне забезпечення, що містить реалізацію нового криптографічного алгоритму(-ів), який відмінний від реалізованого(-их) виробником засобу КЗІ і взаємодіє з СПЗ об-

робки запитів на виконання криптографічних перетворень від внутрішніх програмних застосувань, записаних у засіб КЗІ на попередньому етапі, завантажено на другому етапі СПЗ також взаємодіє із зовнішніми по відношенню до засобу КЗІ термінальними програмними застосуваннями, які потребують виконання криптографічних перетворень відповідно до реалізованого нового криптографічного алгоритму.

2. Спосіб за п. 1, який **відрізняється** тим, що записують спеціальне програмне забезпечення, яке взаємодіє з базовим програмним забезпеченням виробника (операційною системою пристрою, наприклад SMART-картою або USB криптографічного токена) і використовує реалізовані в постійній пам'яті засобу КЗІ криптографічні примітиви (математичні операції), прошиті в масці постійного запам'ятовуючого пристрою і необхідні для виконання криптографічних перетворень, передбачених криптографічним алгоритмом.

3. Спосіб за п. 2, який **відрізняється** тим, що записують спеціальне програмне забезпечення, яке використовує криптографічні примітиви (математичні операції), реалізовані в спеціалізованому криптографічному процесорі/співпроцесорі.

4. Спосіб за п. 1, який **відрізняється** тим, що записують спеціальне програмне забезпечення, яке взаємодіє із засобом КЗІ, виготовленим у вигляді окремого комп'ютерного блока/плати - апаратного модуля безпеки HSM, при цьому спеціальне програмне забезпечення реалізують у вигляді функціонального модуля FM, спеціально призначеного для подібних HSM-пристроїв.

Корисна модель належить до апаратних, програмно-апаратних засобів криптографічного захисту інформації (криптографічний засіб, КЗІ). Технічний результат полягає в можливості застосування нових криптографічних алгоритмів (механізмів) на базі математичних криптографічних операцій (криптографічних примітивів), реалізованих виробником у конкретному засобі КЗІ та призначених для використання інших криптографічних алгоритмів (механізмів) без внесення будь-яких змін у про-

грамне забезпечення виробника.

За допомогою певного інтерфейсу програмно-го забезпечення (операційної системи) виробника, що одноразово додається до системи внутрішніх операцій засобу КЗІ, реалізуються нові криптографічні алгоритми, що дозволяє забезпечити універсальність використання засобу КЗІ та сферу його застосування.

Одним з найбільш відомих у даний час способів використання засобів КЗІ є застосування крип-

UA (19)
UA (11) 66790 (13) U

тографічних алгоритмів (механізмів), таких як AES, DES, 3DES, RSA, ECDSA та інш., закладених виробником у постійній пам'яті пристрою, наприклад, прошитих у масці постійного запам'ятовуючого пристрою (ПЗП) (ROM, англ. Read Only Memory). Однак актуальною є можливість використання КЗІ для подібних, але не ідентичних, до реалізованих виробником криптографічних алгоритмів, шляхом створення спеціального програмного забезпечення (СПЗ), наприклад, на рівні електронно - перепрограмованої постійної пам'яті (ППЗУ) (EEPROM, англ. Electrically Erasable Programmable Read Only Memory). Цим самим існуючий засіб КЗІ набуває нової функціональності та області застосування за рахунок можливості використання нових, нереалізованих виробником, криптографічних алгоритмів, наприклад, ГОСТ 34.10-2001, ДСТУ 4145-2002 та інш.

Слід відмітити, що значна кількість технічних рішень була розроблена для реалізації певного ряду криптографічних алгоритмів, вбудованих виробником у засіб КЗІ на стадії виробництва. Більшість реалізованих технічних рішень орієнтовано на застосування конкретних міжнародних криптографічних алгоритмів, тому вони не можуть бути безпосередньо застосовані для криптографічних перетворень нових (національних) криптографічних алгоритмів.

Запропонована корисна модель дозволяє створити, використовуючи криптографічні примітиви засобу КЗІ, та завантажити у засіб КЗІ програмну реалізацію нових криптографічних алгоритмів електронного цифрового підпису (ЕЦП), автентифікації, шифрування тощо, які відрізняються від реалізованих у цих засобах виробником під час стадії виробництва. Застосування корисної моделі для створення нового покоління криптографічних засобів з розширеною функціональністю (наприклад, з використанням криптографічних примітивів на еліптичних кривих над простим полем EC Fp та кінцевим полем EC F2m) дозволить без витрат на розробку та створення пристроїв для кожного нового криптографічного алгоритму (наприклад, ГОСТ 34.10-2001 чи ДСТУ 4145-2002 та інших) використовувати ці засоби КЗІ для різних додатків та сервісів (бізнес-сектор, банківський сектор, державний сектор) із застосуванням національних криптографічних алгоритмів, що є державними стандартами України (ДСТУ 4145-2002), Росії та країн СНД (ГОСТ Р 34.10, ГОСТ 34.311), а також алгоритмів, розроблених в інших країнах. Таким чином, зазначені засоби КЗІ із програмним забезпеченням, що реалізує запропонований спосіб, можуть застосовуватися не тільки у країнах, де використовуються традиційні міжнародні криптографічні алгоритми, але й для ряду країн, що мають національні криптографічні алгоритми, наприклад, країн колишнього СРСР та інш.

У патенті США 0075254 [1] описується спосіб розширення функціональності СМАРТ-карти за рахунок використання співпроцесора безпеки, включеного у пристрій. Внутрішній закритий (персональний) ключ міститься в енергонезалежному ПЗП співпроцесора безпеки та використовується для шифрування даних СМАРТ-картою, які збері-

гають у зовнішній пам'яті. Внутрішній оперативний запам'ятовуючий пристрій (ОЗП) для обробки даних є доступним тільки співпроцесору безпеки. Блоки даних, збережені в зовнішній пам'яті, зашифровують та розшифровують з використанням закритого ключа. Якщо інші секретні або симетричні ключі включені в блок даних, то вони після розшифрування закритим внутрішнім ключем, зберігаються у відкритому вигляді у внутрішньому ОЗП. Центральний процесор (ЦП) може запросити співпроцесор безпеки зашифрувати/розшифрувати дані, використовуючи інші секретні або симетричні ключі, що зберігаються у внутрішньому ОЗП. Недоліком даного методу є використання криптографічних функцій зашифрування та розшифрування даних і тільки на алгоритмах, закладених у ПЗП пристрою виробником.

У викладеній патентній заявці Росії 2010110344 [2] пропонується спосіб криптографічної обробки інформації з використанням криптографічного процесора, який містить один або декілька арифметико-логічних пристроїв (ALU) і множину регістрів даних. На першому етапі приймають блок даних α -бітової довжини, причому блок даних організований як α/n n -бітових слів. Далі α/n n -бітових слів зберігають як структуру в регістрах даних, причому кожне n -бітове слово даних зберігається у відповідному n -бітовому елементі структури. Потім здійснюють перетворення перемішуванням стовпців у структурі з використанням одного або декількох ALU, причому перетворення перемішуванням стовпців припускає формування добутків кінцевого поля з використанням побітового зсуву та операцій виключного АБО (XOR). Недоліком цього способу є його висока обчислювальна складність і реалізація тільки криптографічного алгоритму шифрування/розшифрування даних AES.

У патенті США 7278582 [3] розглядається спосіб реалізації апаратного модуля безпеки (HSM, англ. Hardware Security Module), заснований на застосуванні чип-карти зі схемою обробки, що функціонує відповідно до набору команд, які зберігаються в пам'яті чип-карти. Спосіб також містить у собі операції для завантаження набору команд, що реалізують криптографічний стандарт шифрування з відкритим ключем PKCS#11. PKCS - криптографічні стандарти відкритого ключа (англ. Public Key Cryptography Standards). Чип-карта взаємодіє із сервером, настроєним для роботи у відповідності зі стандартом PKCS#11.

Спосіб забезпечує роботу в мережі сервера та мережних об'єктів, які є зовнішніми стосовно сервера та чип-карти. У пам'яті чип-карти (Java-карти) завантажують набір інструкцій, який призначений для використання стандарту PKCS#11. Java-карта, містить один або декілька аплетів, що завантажують у ППЗУ, для забезпечення функціонування з PKCS#11 - сумісними пристроями. Далі завантажують набір команд для взаємодії чип-карти із сервером, який працює відповідно до PKCS#11. Недоліком даного способу є застосування обмеженого набору криптографічних операцій (генерація майстра-ключа і його зберігання у

пам'яті чип-карти) та реалізація тільки алгоритму RSA.

З відомих способів застосування криптографічних алгоритмів у криптографічних засобах захисту інформації найбільш близьким за технічною суттю до винаходу є патент США 7986786 [4], який описує спосіб використання криптографічних функцій, наданих криптографічним співпроцесором. Даний спосіб дозволяє об'єктам платформи, таким як Базова система вводу-виводу (BIOS) вибірково використовувати криптографічні функції криптографічного співпроцесора. Недоліком способу є те, що спеціальне програмне забезпечення, що реалізує криптографічні примітиви, розміщено в співпроцесорі пристрою, тому можуть бути використані тільки закладені виробником криптографічні алгоритми, зокрема RSA (SHA-1, HMAC та інш.).

Задачею корисної моделі є застосування способу використання криптографічних алгоритмів на доповнення до вбудованих/прошитих у засобі КЗІ виробником (наприклад, у масці ГТЗП) на стадії виробництва для реалізації різних криптографічних функцій: цифрового підпису, аутентифікації, геш-функцій, генерації ключів, шифрування та інш. У засіб КЗІ на стадії виробництва або підготовки його до експлуатації записують спеціальне програмне забезпечення, у якому з використанням криптографічних примітивів засобу КЗІ, реалізують додаткові до вбудованих у засіб криптографічні алгоритми генерації ключів, формування та перевірки ЕЦП, вироблення геш-значень тощо, які згодом використовуються зовнішніми застосуваннями. СПЗ розробляється та реалізується за допомогою спеціалізованих програмних бібліотек криптографічних примітивів розробника, наданих виробником засобу КЗІ.

Поставлена задача вирішується за рахунок того, що спосіб застосування криптографічних алгоритмів у засобах захисту інформації полягає у тому, що застосовують криптографічні алгоритми, вбудовані виробником на стадії виробництва або підготовки його до експлуатації для реалізації криптографічних функцій, згідно з корисною моделлю, складається з наступних етапів:

записують спеціальне програмне забезпечення, у якому реалізують обробку запитів від внутрішніх програмних застосувань на виконання криптографічних перетворень у відповідності до алгоритмів, закладених виробником пристроїв або створених за правилами, передбаченими виробником для інших криптографічних алгоритмів;

у засіб КЗІ записують спеціальне програмне забезпечення, що містить реалізацію нового криптографічного алгоритму(-ів), який відмінний від реалізованого(-их) виробником засобу КЗІ і взаємодіє з СПЗ обробки запитів на виконання криптографічних перетворень від внутрішніх програмних застосувань, записаних у засіб КЗІ на попередньому етапі. Завантажене на другому етапі СПЗ також взаємодіє із зовнішніми по відношенню до засобу КЗІ термінальними програмними застосуваннями, які потребують виконання криптографічних перетворень відповідно до реалізованого нового криптографічного алгоритму.

Записують спеціальне програмне забезпечен-

ня, яке взаємодіє з базовим програмним забезпеченням виробника (операційною системою пристрою, наприклад, СМАРТ-картою або USB криптографічного токена) і використовує реалізовані в постійній пам'яті засобу КЗІ криптографічні примітиви (математичні операції), прошиті в масці постійного запам'ятовуючого пристрою і необхідні для виконання криптографічних перетворень, передбачених криптографічним алгоритмом.

Записують спеціальне програмне забезпечення, яке використовує криптографічні примітиви (математичні операції), реалізовані в спеціалізованому криптографічному процесорі/співпроцесорі.

Записують спеціальне програмне забезпечення, яке взаємодіє із засобом КЗІ, виготовленим у вигляді окремого комп'ютерного блока/плати - апаратного модуля безпеки HSM. Спеціальне програмне забезпечення реалізують у вигляді функціонального модуля (FM, англ. Functionality Module), спеціально призначеного для подібних HSM-пристроїв.

Це дозволяє істотно розширити функціональність вже існуючих засобів КЗІ для створення нового покоління засобів.

На кресленні (фіг. 1) зображена структурна блок-схема реалізації способу використання криптографічних алгоритмів у засобах криптографічного захисту інформації.

Спосіб застосування криптографічних алгоритмів у засобах КЗІ складається з наступних етапів:

До засобу КЗІ записують СПЗ, у якому реалізують обробку запитів від внутрішніх програмних застосувань на виконання криптографічних перетворень у відповідності до алгоритмів, закладених виробником пристроїв або створених за правилами, передбаченими виробником для інших криптографічних алгоритмів.

Далі до засобу КЗІ записують спеціальне програмне забезпечення, що містить реалізацію нового криптографічного алгоритму(-ів), який відрізняється від реалізованого(-их) виробником засобу КЗІ і взаємодіє з СПЗ обробки запитів на виконання криптографічних перетворень від внутрішніх програмних застосувань, записаних у засіб КЗІ на попередньому етапі. Завантажене на другому етапі СПЗ також взаємодіє із зовнішніми по відношенню до засобу КЗІ термінальними програмними застосуваннями, які потребують виконання криптографічних перетворень відповідно до реалізованого нового криптографічного алгоритму.

Записують спеціальне програмне забезпечення, яке взаємодіє з базовим програмним забезпеченням виробника (операційною системою пристрою, наприклад, СМАРТ-картою або USB криптографічного токена) і використовує реалізовані в постійній пам'яті засобу КЗІ криптографічні примітиви (математичні операції), прошиті в масці постійного запам'ятовуючого пристрою і необхідні для виконання криптографічних перетворень, передбачених криптографічним алгоритмом.

Записують спеціальне програмне забезпечення, яке використовує криптографічні примітиви, реалізовані в спеціалізованому криптографічному процесорі/співпроцесорі.

Записують спеціальне програмне забезпечення, яке взаємодіє із засобом КЗІ, виготовленим у вигляді окремого комп'ютерного блока/плати - апаратного модуля безпеки HSM. Спеціальне програмне забезпечення реалізують у вигляді функціонального модуля FM, спеціально призначеного для подібних HSM-пристроїв.

Креслення (фіг. 2) відображає алгоритмічну схему застосування способу в засобах КЗІ для використання різних криптографічних алгоритмів.

На кресленні (фіг. 3) зображена структурна блок-схема реалізації способу використання криптографічних алгоритмів у криптографічних засобах захисту інформації у вигляді SMART-карти або

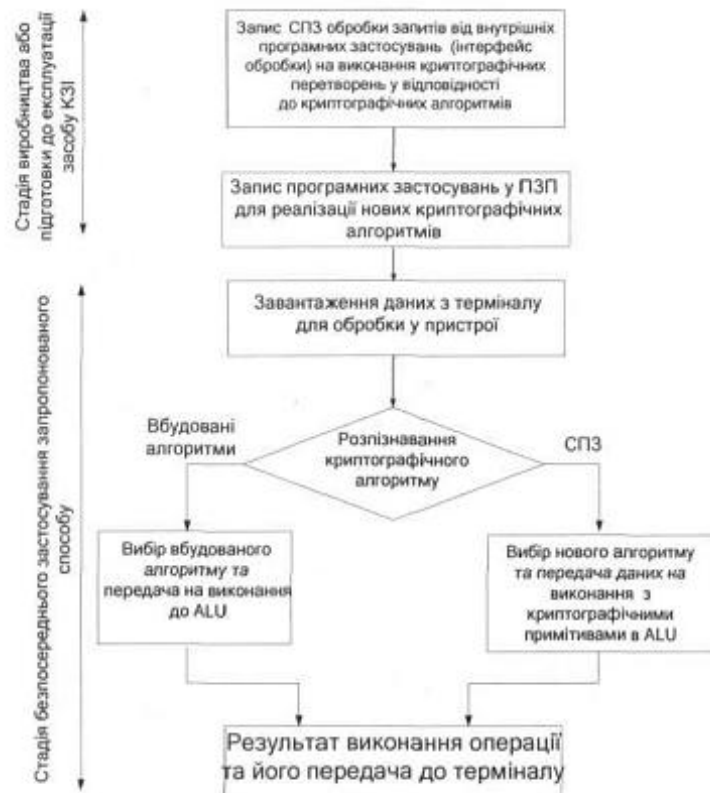
USB криптографічного токена. Внутрішні програмні застосування, у тому числі спеціальне програмне забезпечення, можуть бути записані як у ГШЗУ, так безпосередньо і у ПЗП засобу КЗІ.

Джерела інформації:

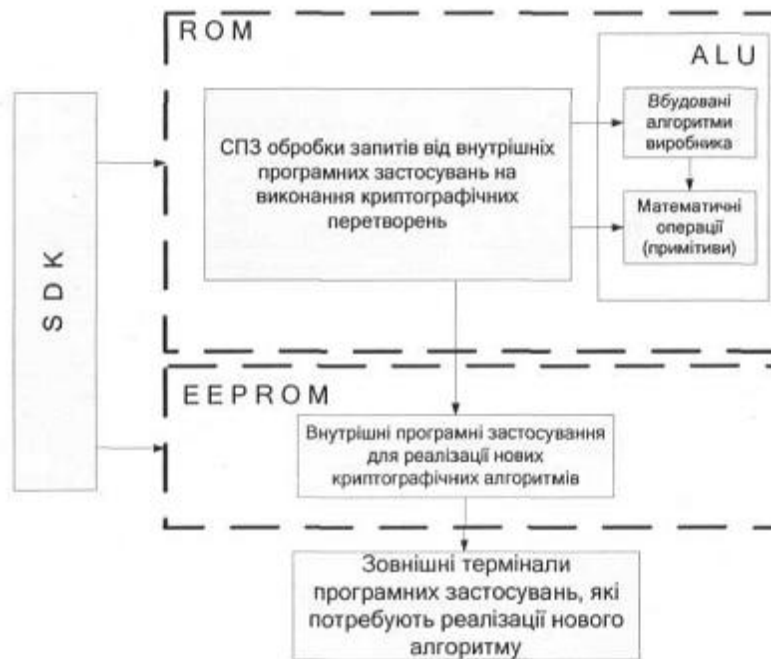
1. Патент США № 0075254, МПК H04D1/00, 2006
2. Заявка на винахід РФ № 2010110344/08, МПК G09C5/00, 2010
3. Патент США № 7278582, МПК G06D19/06, 2007
4. Патент США № 7986786, МПК H04L9/00, 2011



Фіг. 1



Фіг. 2



Фіг. 3

