



УКРАЇНА

(19) UA (11) 63213 (13) U  
(51) МПК (2011.01)  
G09C 5/00  
G11C 8/00

ДЕРЖАВНА СЛУЖБА  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ  
УКРАЇНИ

## ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під  
відповідальність  
власника  
патенту

(54) ПРИСТРІЙ ДЛЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ "IBANK 2 KEY"

1

(21) u201109709  
(22) 03.08.2011  
(24) 26.09.2011  
(46) 26.09.2011, Бюл.№ 18, 2011 р.  
(72) ФАДЕЄВ ОЛЕКСАНДР БОРИСОВИЧ  
(73) ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДА-  
ЛЬНІСТЮ "БІФІТ СЕРВІС"  
(57) Пристрій для криптографічного захисту інфо-  
рмації, що виконаний у вигляді малогабаритного  
USB-пристрою і складається з корпусу (1), в якому  
на друкованій платі (2) розміщені USB-роз'єм (3)  
підвищеної довговічності, мікроконтролер (4), блок  
(5) енергонезалежної пам'яті і модуль (7) світлоді-  
одної індикації для сигналізації підключення при-  
строю до електронного порту (9) USB електронно-  
обчислювальної машини (EOM) (8), а контакти

2

USB-роз'єму (3) підвищеної довговічності і модуль  
(7) світлової індикації підключені до мікроконтро-  
лера (4), який **відрізняється** тим, що додатково  
містить модуль (6) генерації випадкових чисел,  
який підключений до мікроконтролера (4), а блок  
(5) енергонезалежної пам'яті розташований усе-  
редині мікроконтролера (4) і має механізм захисту  
від зчитування, причому модуль (7) світлодіодної  
індикації виконаний з можливістю відображення  
події взаємодії EOM (8) з пристроєм, USB-роз'єм  
(3) підвищеної довговічності виконаний по індиві-  
дуальній схемі з односторонніми клямками, на які  
кріпиться корпус (1) пристрою, і містить суцільно-  
металевий каркас, який зафіксований на друкова-  
ній платі (2) металевими утримувачами.

Корисна модель належить до галузі техніки по  
захисту інформації, в тому числі може бути вико-  
ристана в пристроях для запобігання несанкціоно-  
ваного доступу до інформаційних ресурсів конфі-  
денційного призначення: паролем, цифровим  
сертифікатам, ключам шифрування і електронного  
цифрового підпису.

З рівня техніки відомі пристрої для генерації  
ключової інформації та захищеного зберігання  
інформації з обмеженим доступом, які виконані у  
вигляді малогабаритного USB-пристрою, що скла-  
даються з корпусу, в якому на друкованій платі  
розміщені USB-роз'єм і мікроконтролер [USB-токен  
Кристал-1, ЗАТ "Інститут інформаційних техноло-  
гій", м. Харків, вул. Бакуліна 12, ліцензія АВ  
№501777 від 17.02.2010 на діяльність по крипто-  
графічному захисту інформації, яка складає дер-  
жавну таємницю, конфіденційної інформації, яка є  
власністю держави, конфіденційної інформації;  
ліцензія АВ №340168 від 11.07.2007 на діяльність  
по технічному захисту інформації всіх видів (ана-  
лог)] [1]; [USB-токен SECURE TOKEN, ТОВ "Ав-  
тор", м. Київ, вул. Смоленська 31-33, ліцензія АВ  
№720275 від 19.05.2005 на діяльність по крипто-  
графічному захисту конфіденційної інформації, яка  
є власністю держави, конфіденційної інформації;

ліцензія АВ №307838 від 22.03.2007, на діяльність  
по технічному захисту інформації, яка не є держа-  
вною таємницею (аналог)] [2].

У відомих пристроях [1,2] реалізовано шифру-  
вання згідно ДСТУ ГОСТ 28147:2009, електронний  
цифровий підпис (ЕЦП) згідно ДСТУ 4145-2002,  
гешування згідно ГОСТ 34.311-95, протокол роз-  
поділу ключових даних Діффі-Гелмана в групі то-  
чок еліптичної кривої згідно ДСТУ ISO/IEC15946-  
3:2006.

Апаратна реалізація відомих пристроїв для ге-  
нерації ключової інформації та захищеного збері-  
гання інформації з обмеженим доступом забезпе-  
чує захищеність процесу виконання  
криптографічних перетворень і робить неможли-  
вим доступ до особистих ключів з боку зовнішньо-  
го апаратно-програмного середовища.

У наведених пристроях особисті ключі генеру-  
ються, зберігаються і використовуються тільки  
усередині пристрою, і не за яких обставин не пот-  
рапляють за його межі.

Недоліки відомих пристроїв [1,2] полягають у  
малій кількості ключів, що зберігаються, низькій  
швидкості виконання криптографічних операцій,  
відсутності підтримки усіх розповсюджених ОС.

(19) UA (11) 63213 (13) U

З рівня техніки також відомий найбільш близький по технічній суті до корисної моделі, що заявляється, пристрій для криптографічного захисту інформації - ідентифікатор RUTOKEN, який виконаний у вигляді малогабаритного USB-пристрою і складається з корпусу, в якому на друкованій платі розміщені USB-роз'єм підвищеної довговічності, мікроконтролер, блок енергонезалежної пам'яті і модуль світлодіодної індикації для сигналізації підключення пристрою до електронного порту електронно-обчислювальної машини (ЕОМ), а контакти USB-роз'єму підвищеної довговічності і модуль світлової індикації підключені до мікроконтролера [Ідентифікатор RUTOKEN, Компанія "Актив", м. Москва, вул. Красіна, д.3, Ліцензія ФСТЕК РФ №0415 від 05.12.2005 на діяльність по технічному захисту конфіденційної інформації (прототип)] [3].

Після того, як ідентифікатор RUTOKEN встановлено в USB-електронний порт ЕОМ і світлодіодний індикатор підтвердив факт підключення, оператор набирає на ЕОМ необхідний PIN-код для подальшого доступу до інформаційних ресурсів.

Недолік відомого пристрою [3] полягає в тому, що ідентифікатор RUTOKEN не підтримує національні криптографічні стандарти формування/перевіряння ЕЦП ДСТУ 4145-2002, розподілу ключових даних Діффі-Гелмана в групі точок еліптичної кривої ДСТУ ISO/IEC15946-3:2006.

Крім того, у відомому пристрої [3] не реалізований апаратний генератор випадкових чисел, що погіршує криптостійкість ключової інформації, що генерується на пристрої.

А для зберігання конфіденційних даних використовується зовнішня енергонезалежна пам'ять, що створює загрозу несанкціонованого доступу до конфіденційних даних, оскільки зовнішня енергонезалежна пам'ять не має захисту від зчитування даних.

Задачею корисної моделі є удосконалення пристрою для криптографічного захисту інформації так, щоб забезпечити підтримку національних криптографічних стандартів, поліпшити показники швидкості шифрування, гешування та формування ЕЦП, збільшити кількість особистих ключів, що зберігаються у пристрої, підвищити рівень безпеки пристрою, а саме підвищити криптостійкість ключової інформації, що генерується на пристрої та знизити загрозу несанкціонованого доступу до конфіденційних даних, а також покращити міцність пристрою, забезпечити підтримку всіх сучасних операційних систем і відсутність необхідності власноруч встановлювати драйвери.

Поставлена задача вирішується тим, що пристрій для криптографічного захисту інформації, що виконаний у вигляді малогабаритного USB-пристрою і складається з корпусу, в якому на друкованій платі розміщені USB-роз'єм підвищеної довговічності, мікроконтролер, блок енергонезалежної пам'яті, і модуль світлодіодної індикації для сигналізації підключення пристрою до електронного порту ЕОМ, а контакти USB-роз'єму і модуль світлової індикації підключені до мікроконтролера, згідно з корисною моделлю, додатково містить модуль генерації випадкових чисел, який підключений до мікроконтролера, а блок незалежної па-

м'яті розташований усередині мікроконтролера, причому модуль світлодіодної індикації виконаний з можливістю відображення події взаємодії ЕОМ з пристроєм, USB-роз'єм підвищеної довговічності виконаний по індивідуальній схемі і містить суцільнометалевий каркас, який зафіксований на друкованій платі металевими утримувачами.

У зв'язку з тим, що пропонований пристрій додатково містить модуль генерації випадкових чисел, який підключений до мікроконтролера, при генерації ключової інформації вноситься додатковий шум, що підвищує криптостійкість ключової інформації.

Завдяки тому, що модуль світлодіодної індикації виконано з додатковим функціоналом, досягається можливість інформування оператора про факт взаємодії ЕОМ з пристроєм.

За рахунок того, що USB-роз'єм підвищеної довговічності виконаний по індивідуальній схемі і містить суцільнометалевий каркас, який зафіксований на друкованій платі металевими утримувачами, суттєво підвищується надійність і довговічність пристрою, оскільки корпус пристрою кріпиться до USB-роз'єму за допомогою односторонніх клямок, які при першій фіксації корпусу не дозволяють більше його знімати без його фізичного пошкодження, що сигналізує про навмисний злом пристрою.

Надалі корисна модель пояснюється прикладом її здійснення з посиланням на креслення, що додаються.

На Фіг.1 зображена функціональна схема пристрою для доступу до конфіденційної інформації, виконаного у вигляді малогабаритного USB-пристрою.

На Фіг.2 зображений пристрій для доступу до конфіденційної інформації, виконаний у вигляді малогабаритного USB-пристрою, фото з двох сторін, без корпусу.

На Фіг.3 зображений пристрій для доступу до конфіденційної інформації, виконаний у вигляді малогабаритного USB-пристрою, фото, з корпусом.

Пристрій для доступу до конфіденційної інформації, виконаний у вигляді малогабаритного USB-пристрою (Фіг.1, 2, 3), складається (Фіг.1) з корпусу 1, в якому на друкованій платі 2 розміщені USB-роз'єм 3 підвищеної довговічності, мікроконтролер 4, блок 5 енергонезалежної пам'яті, і модуль 7 світлодіодної індикації для сигналізації підключення пристрою до електронного порту 9 ЕОМ 8, а контакти USB-роз'єму 3 і модуль 7 світлової індикації підключені до мікроконтролера 4.

Головними особливостями вдосконаленого пристрою для криптографічного захисту інформації, виконаного у вигляді малогабаритного USB-пристрою, є те, що він додатково містить модуль 6 генерації випадкових чисел, який підключений до мікроконтролера 4, а блок 5 енергонезалежної пам'яті розташований усередині мікроконтролера 4 і має захист від зчитування, модуль 7 світлодіодної індикації виконаний з можливістю відображення події взаємодії ЕОМ 8 з пристроєм, USB-роз'єм 3 підвищеної довговічності виконаний за індивідуальною схемою і містить суцільнометале-

вий каркас, який зафіксований на друкованій платі 2 металевими утримувачами, корпус 1 пристрою кріпиться до USB-роз'єму 3 за допомогою односторонніх клямок, які при першій фіксації корпусу 1 не дозволяють більше його знімати без його фізичного пошкодження, що сигналізує про навмисний злом пристрою.

Корпус 1 пристрою виконаний, переважно зі світлопрозорої пластмаси, наприклад зі світлопрозорого полікарбонату.

Пропонований пристрій працює таким чином.

При підключенні пристрою за допомогою USB-роз'єму 3 підвищеної довговічності, виконаного із спеціальними металевими утримувачами, до електричних контактів електронного порту 9 EOM 8 виконується ініціалізація мікроконтролера 4, модуля 6 генерації випадкових чисел і модуля 7 світлової індикації.

У разі успіху ініціалізації пристрою спрацьовує модуль 7 світлодіодної індикації, який інформує оператора про факт успішного підключення пристрою до EOM 8.

Після успішного підключення оператор може взаємодіяти з пристроєм: виконувати криптографічні операції, операції з файловою системою.

Для деяких операцій потрібна автентифікація оператора, для чого оператор EOM 8 за допомогою клавіатури EOM 8 вводить PIN-код.

Під час виконання операцій з пристроєм, модуль 7 світлодіодної індикації сигналізує про кожну взаємодію з пристроєм, за рахунок чого забезпечується візуальний контроль взаємодії з пристроєм.

Для деяких криптографічних операцій потрібно згенерувати ключову інформацію.

Для підвищення захищеності генерації випадкових чисел використовується додаткове джерело випадковості - модуль 6 генерації випадкових чисел.

Модуль 6 генерації випадкових чисел реалізований як два незалежні апаратні датчики випадкових чисел (ДВЧ).

Для роботи ДВЧ необхідний сигнал широкоімпульсної модуляції (PWM) частотою порядку 30 кГц.

На виході ДВЧ формується сигнал із сплесками рівня логічної "1" із заздалегідь невідомими довжиною сплеску і інтервалами між ними.

Модуль генерації випадкових чисел, як випадкову величину використовує інтервали часу між передніми фронтами станів логічної "1" з ДВЧ.

Для обробки сигналів з ДВЧ використовується механізм переривань.

Переривання виникають по передньому фронту імпульсів.

Знімання випадковості проводиться послідовно спочатку з одного ДВЧ, а потім з іншого.

У разі несправності одного з ДВЧ, він не бере участь в генерації випадкового числа.

У разі несправності обох ДВЧ додаткова випадковість при генерації ключової інформації не домішується.

Випадковість, що знімається, з ДВЧ є інтервалом часу між двома послідовними перериваннями,

обчислюваним як різниця станів лічильника таймера, у момент виникнення переривань.

Від отриманого 2-х байтового значення інтервалу береться тільки молодший байт.

У разі виникнення переповнювання лічильника таймера проводиться компенсація перенесення при обчисленні різниці.

Дослідним шляхом було визначено, що ентропія одного байта отриманого від ДВЧ складає не менше 7 біт, з кожного ДВЧ знімається по 2688 байт, після чого випадкові байти піддаються процедурі перемішування, на виході якої виходять 40 випадкових байт.

За один цикл генерується 32 випадкових байт.

Час генерації 32 випадкових байт - 0,1 с.

Таким чином, шляхом встановлення на друковану плату модуля генерації випадкових чисел підвищилась криптостійкість ключової інформації, що генерується на пристрої, розташування модуля енергонезалежної пам'яті усередині мікроконтролера знизилась загроза несанкціонованого доступу до конфіденційних даних, використання USB-роз'єму підвищеної довговічності, виконаного по індивідуальній схемі, з односторонніми клямками на які кріпиться корпус пристрою, покращилась міцність пристрою, що взагалі, дозволило реалізувати у пристрої підтримку національних криптографічних стандартів, поліпшити показники швидкості шифрування, гешування та формування ЕЦП, збільшити кількість особистих ключів та забезпечити підтримку всіх сучасних операційних систем і відсутність необхідності власноруч встановлювати драйвери.

У організації - заявнику був виготовлений дослідний зразок - пристрій для криптографічного захисту інформації, виконаний у вигляді малогабаритного USB-пристрою (Фіг.2, 3), реалізовано програмне забезпечення, яке записується на блок 5 енергонезалежної пам'яті і виконується мікроконтролером 4.

Дослідний зразок було протестовано на стендах організації.

В результаті тестування було підтверджено, що пристрій виконує вимоги, що вище висуваються до нього:

1. Реалізує державні криптографічні стандарти: ДСТУ ГОСТ 28147:2009, ДСТУ 4145-2002, ГОСТ 34.311-95 і ДСТУ ISO/IEC15946-3:2006. Реалізує генерацію і зберігання особистих ключів ЕЦП, що запобігає несанкціонованому доступу до ключа з боку зовнішнього апаратно-програмного середовища;

2. Дозволяє згенерувати і зберегти до 64-х особистих ключів ЕЦП. Містить додатково 48 Кб пам'яті для захищеного зберігання даних користувача;

3. Підтверджено, що ентропія одного випадкового байта отриманого з ДВЧ складає не менше 7 біт;

4. Має високі показники швидкості виконання криптографічних операцій: формування ЕЦП - 54 мс, перевірка ЕЦП - 174 мс, формування загального секрету по схемі Діффі-Гелмана - 168 мс, шифрування, обчислення имитовставки і геш-вектора - близько 1 Мбіт/с.

5. Підтримується в ОС Windows, Linux і Mac OS X.

Пристрій для криптографічного захисту інформації, виконаний у вигляді малогабаритного USB-токена, з вказаним програмним забезпеченням проходив перевірку в експертній лабораторії ДССЗІ України, внаслідок чого було отримано експертний висновок №05/1-1147 ДССЗІ України від 30.03.11.

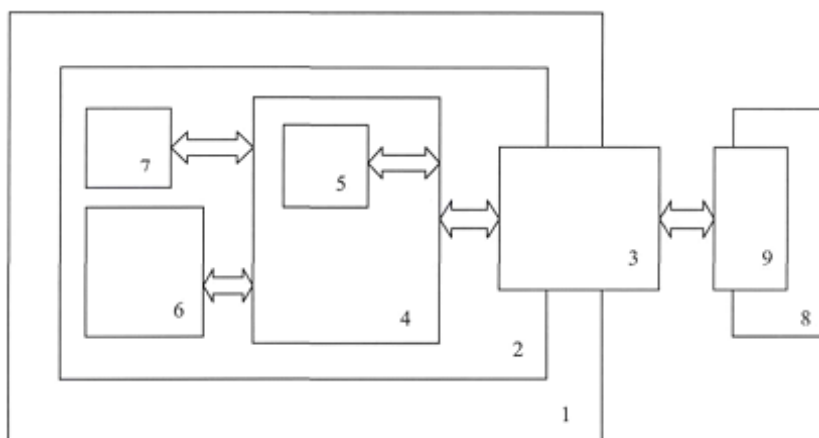
Згідно з експертним висновком, криптографічні алгоритми, реалізовані в "iBank2Key", відповідають вимогам стандартів ДСТУ ГОСТ 28147:2009, ДСТУ 4145-2002, ГОСТ 34.311-95 і ДСТУ ISO/IEC15946-3:2006.

Наведені відомості підтверджують можливість промислового застосування пропонованого пристрою для криптографічного захисту інформації,

виконаного у вигляді малогабаритного USB-пристрою, який може знайти широке застосування в сфері захисту інформації, наприклад для запобігання несанкціонованого доступу до інформаційних ресурсів таких як: паролі, цифрові сертифікати, ключі шифрування і ЕЦП.

Перелік позначень

1. Корпус.
2. Друкована плата.
3. USB-роз'єм підвищеної довговічності.
4. Мікроконтролер.
5. Блок енергонезалежної пам'яті, що має механізм захисту від зчитування.
6. Модуль генерації випадкових чисел.
7. Модуль світлової індикації.
8. EOM.
9. Електронний USB-порт EOM.



Фиг.1



Фиг.2



Фиг.3