



УКРАЇНА

(19) **UA** (11) **76828** (13) **U**  
(51) МПК (2013.01)  
**G06F 21/00**  
**H04L 9/32** (2006.01)

ДЕРЖАВНА СЛУЖБА  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ  
УКРАЇНИ

**(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ**

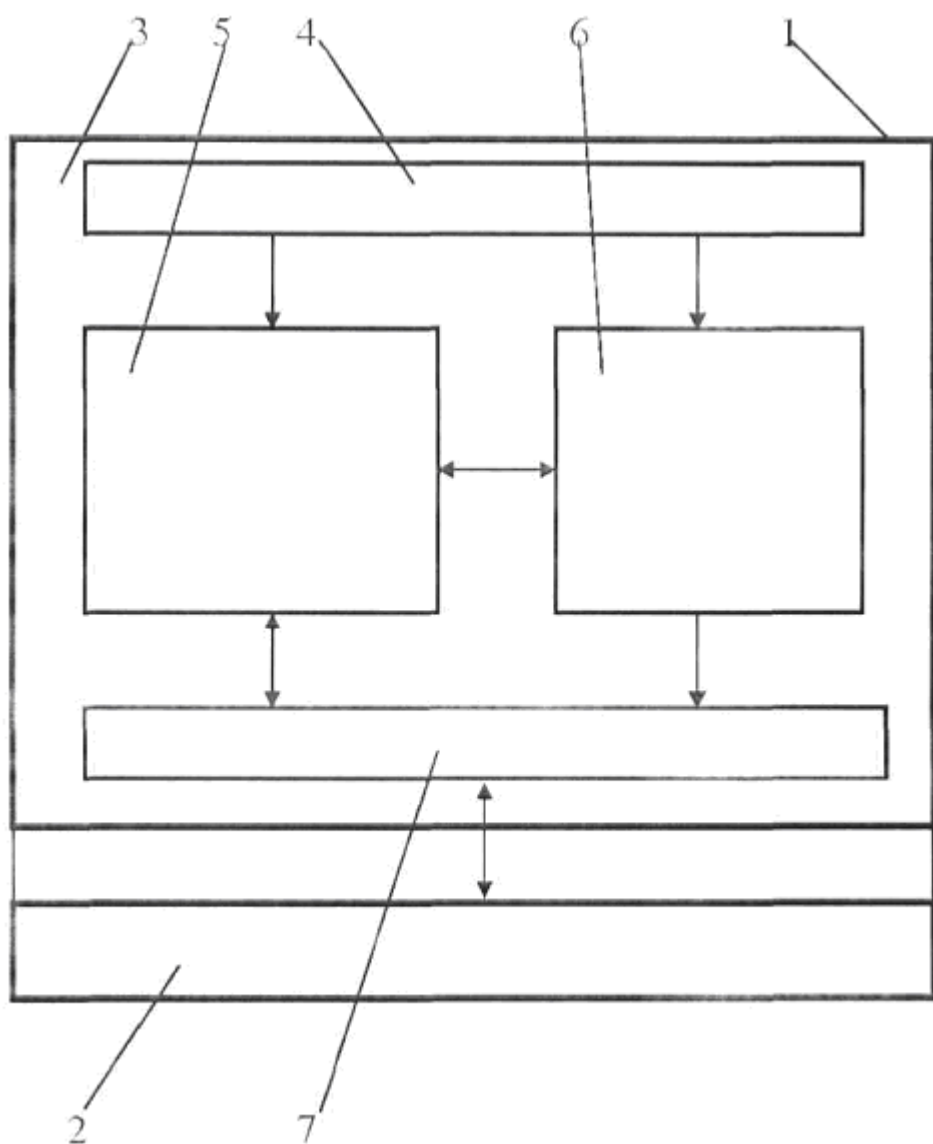
<b>(21)</b> Номер заявки: <b>u 2012 12659</b>	<b>(72)</b> Винахідник(и): <b>Рудюк Сергій Анатолійович (UA)</b>
<b>(22)</b> Дата подання заявки: <b>05.11.2012</b>	<b>(73)</b> Власник(и): <b>Рудюк Сергій Анатолійович,</b> вул. Крейсера «Аврора» 1, кв. 122, м. Київ, 03191 (UA)
<b>(24)</b> Дата, з якої є чинними права на корисну модель: <b>10.01.2013</b>	<b>(74)</b> Представник: <b>Ващук Ярослав Петрович, реєстр. №45</b>
<b>(46)</b> Публікація відомостей про видачу патенту: <b>10.01.2013, Бюл.№ 1</b>	

**(54) ПРИСТРІЙ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА ТА ЗАХИСТУ ВІД РЕВЕРС-ІНЖИНІРИНГУ K2-001**

**(57) Реферат:**

Пристрій ідентифікації користувача та захисту від реверс-інжинірингу містить корпус, в якому розміщено мікроконтролер з програмними блоками, порт USB. Блок захисту пам'яті мікроконтролера з'єднаний для обміну даними з блоками алгоритму захисту інформації і енергонезалежної пам'яті, які в свою чергу з'єднані для обміну даними з програмним драйвером, сумісним з USB. Пристрій інтегрований з програмним забезпеченням "Корпорація 2".

UA 76828 U



Корисна модель належить до засобів аутентифікації при користуванні і передачі інформаційних ресурсів з використанням комп'ютерної техніки і мереж, а конкретно, для ідентифікації користувачів в системі з інтегрованими механізмами захисту від злому.

Серед відомих засобів аутентифікації найпоширенішим є аутентифікація по паролю ("Способ и устройство для авторизации санкционированного доступа" патент РФ № 2433471, G06F 21/00, 10.11.2011). Такий метод має суттєві недоліки:

1. Першим і основним недоліком є надійність і безпека пароля користувача:

а) Якщо користувач змінював пароль і приділив недостатньо уваги його надійності, є кілька методів його підібрати. Це так звана "словникова атака" - перебір звичайних слів по словнику, підбір ключа використовуючи інформацію про користувача (ім'я, дата народження тощо), або при короткому паролі можна навіть застосувати прямий перебір всіх варіантів. Для реалізації цих методів існують вже готові програми, які автоматично без втручання за доволі короткий час перебирають всі можливі комбінації простих паролів.

б) Пароль можна також підглянути або перехопити при вводі. Для цього є спеціальні програми — keyLoggers, які в прихованому режимі записують всю інформацію, яка вводиться з клавіатури і навіть за допомогою миші, а потім передають її зловмиснику.

в) Крім того зловмисник може застосувати фізичне насилля для отримання пароля. Або користувач, сам того не знаючи, розкриє в розмові із зловмисником свій пароль — так званий "метод соціальної інженерії".

г) Користувачі можуть передавати іншим людям паролі, тим самим, створюючи загрози інформаційній безпеці.

2. Другим недоліком звичайної аутентифікації є неспроможність користувача розрізнити справжній сервер, до якого він намагається підключитися, від підробленого. На цьому побудовані "фішингові" атаки. Зловмисник підробляє зовнішній вигляд ресурсу (або імітує його роботу), до якого необхідно отримати доступ. А користувач, підключаючись до сервера зловмисника самостійно, нічого не підозрюючи, залишить свої дані аутентифікації. Звісно він не отримає доступу, але цього вже достатньо, щоб зловмисник використав отримані дані для атаки на цільову систему.

3. Третім недоліком є можливість зловмиснику підробляти дані, які передаються користувачем. В такому випадку зловмисник розміщується в розриві каналу зв'язку. Він наскрізно пропускає авторизаційну інформацію, але перехоплює обмін даними і при потребі модифікує їх. Таким чином він може нанести шкоду системі, яку він атакує.

Для уникнення проблем звичайної аутентифікації розробляються різні додаткові методи. Це так звані файли сертифікатів, смарт-карти або USB-токени. Ці прилади дозволяють підключитися до цільової системи, використовуючи ці спеціальні засоби, на яких розміщується додаткова авторизаційна інформація.

Файли сертифікатів, хоча і підвищують безпеку, але не вирішують всіх проблем, оскільки файли можна скопіювати без дозволу власника за допомогою спеціальних шпигунських програм чи під час відсутності власника.

Звичайні смарт-карти і USB-токени (у вигляді носіїв) теж можуть бути скопійовані. Але існують прилади з вбудованим мікроконтролером, які крім збереження сертифікатів дозволяють використовувати спеціальні алгоритми, що дозволяють обмінюватися сертифікатами в неявному вигляді. При чому кожен сеанс обміну може бути унікальним. Це суттєво ускладнює зловмиснику визначити сертифікат. А вбудовані засоби безпеки мікроконтролерів унеможливають отримання сертифікату безпосередньо з приладу.

За прототип прийнято відомий пристрій "Ключ безопасности Secure Token", який виконаний у вигляді USB-брелока, конструкція якого містить корпус з розміщеним в ньому мікроконтролером з програмними блоками та портом USB (інтернет-сайт "Аппаратно-программные средства информационной безопасности" <http://www.author.kiev.ua/data.php?ids=securetoken>). Недоліком конструкції є те, що її програмні блоки та інформаційні канали не забезпечують високу надійність захисту інформації, особливо при передачі через інтернет.

В основу корисної моделі поставлено задачу відому конструкцію пристрою безпеки зробити більш універсальною, розширивши сферу його використання та збільшивши надійність захисту інформації, за рахунок створення нових програмних блоків та з'єднань для обміну даними.

Поставлена задача досягається тим, що в пристрої ідентифікації користувача та захисту від реверс-інжинірингу, що містить корпус, в якому розміщено мікроконтролер з програмними блоками, порт USB, блок захисту пам'яті мікроконтролера з'єднаний для обміну даними з блоками алгоритму захисту інформації і енергонезалежної пам'яті, які в свою чергу з'єднані для обміну даними з програмним драйвером, сумісним з USB.

В свою чергу, пристрій інтегрований з програмним забезпеченням "Корпорація 2".

Вище перераховані нові ознаки (блок захисту пам'яті мікроконтролера, блок алгоритму захисту інформації, блок енергонезалежної пам'яті, програмний драйвер) при взаємодії з відомими ознаками (корпус, в якому розміщено мікроконтролер з програмними блоками, порт USB) забезпечують виявлення нових технічних властивостей корисної моделі і одержання технічного результату: розширення сфери використання та збільшення надійності захисту інформації. В кінцевому результаті отримана можливість покращити споживчі властивості пристрою, пов'язані з технічним результатом, а саме: ідентифікація користувача, захист інформації при передачі через інтернет, а також реалізація дворівневого механізму авторизації користувачів, захист програми "Корпорація 2" від не санкціонованого використання.

На кресленні показана структурна схема пристрою.

Пристрій складається з корпусу 1, в якому розміщено порт USB 2 та мікроконтролер 3, що містить програмні блоки захисту пам'яті 4 мікроконтролера, алгоритму захисту інформації 5, енергонезалежної пам'яті 6 та програмний драйвер 7, сумісний з USB. Контроль і управління пристроєм здійснюється програмним забезпеченням "Корпорація 2".

Пристрій використовують наступним чином.

Після підключення до вільного USB порту комп'ютера пристрій автоматично розпізнається як USB-HID пристрій з назвою K2-001. Для його роботи в системах Windows та Linux не потрібно додаткових драйверів. Коли пристрій розпізнано, він відразу готовий до роботи. Можна запускати програму "Корпорація 2". Пристрій K2-001 містить інформацію про логін користувача, якому виділений цей ключ і термін його дії, а також інформацію про робоче місце (комп'ютер). Ключ прив'язується до персональних даних, що зберігаються в базі даних. Наявність підключеного до комп'ютера ключа свідчить про присутність власника ключа на певному робочому місці.

Для підвищення рівня безпеки використовується так звана двофакторна авторизація. Це означає, що разом з ключем користувач і надалі використовує персональний пароль. Але ключ K2-001 без пароля не дійсний так само як і знання пароля при відсутності ключа не дає доступу до системи.

Пристрій повинен бути підключений протягом всього сеансу зв'язку. При використанні захисту від підробки даних кожна операція забезпечується захистом, сформованим USB ключем K2-001. Окрім цього через певний період часу проводиться повторна авторизація користувача з перевіркою сертифікатів сервера і ключа.

Робота пристрою можлива в наступних режимах:

1. Робота в режимі забезпечення надійної авторизації (аутентифікації).

Під час авторизації ключ обмінюється з сервером сертифікатами за участі програми Корпорація 2 лише як транзитного елемента, який не обробляє самі сертифікати. Таким чином сертифікати не існують на комп'ютері користувача і на будь-яких проміжних вузлах мережі у явному вигляді. Саме це забезпечує надійність цієї схеми авторизації. Крім того ключ має можливість перевірити, що програма дійсно підключилася до сервера Корпорації 2, а не до створеного потенційним зловмисником сервера який імітує роботу сервера Корпорації 2 (так званий фішинг). А сервер аналогічним чином має можливість перевірити сертифікат ключа і визначити його актуальність. Після перевірки сертифікатів ключ K2-001 дає сигнал програмі "Корпорація 2" про успішну перевірку і програма може спокійно продовжувати роботу. Перевірка сертифікатів відбувається через певний інтервал часу. Якщо через певний інтервал часу не відбулося повторної перевірки сертифікатів, сервер розриває з'єднання.

2. Робота в режимі захисту від імітації даних (вироблення імітовставки).

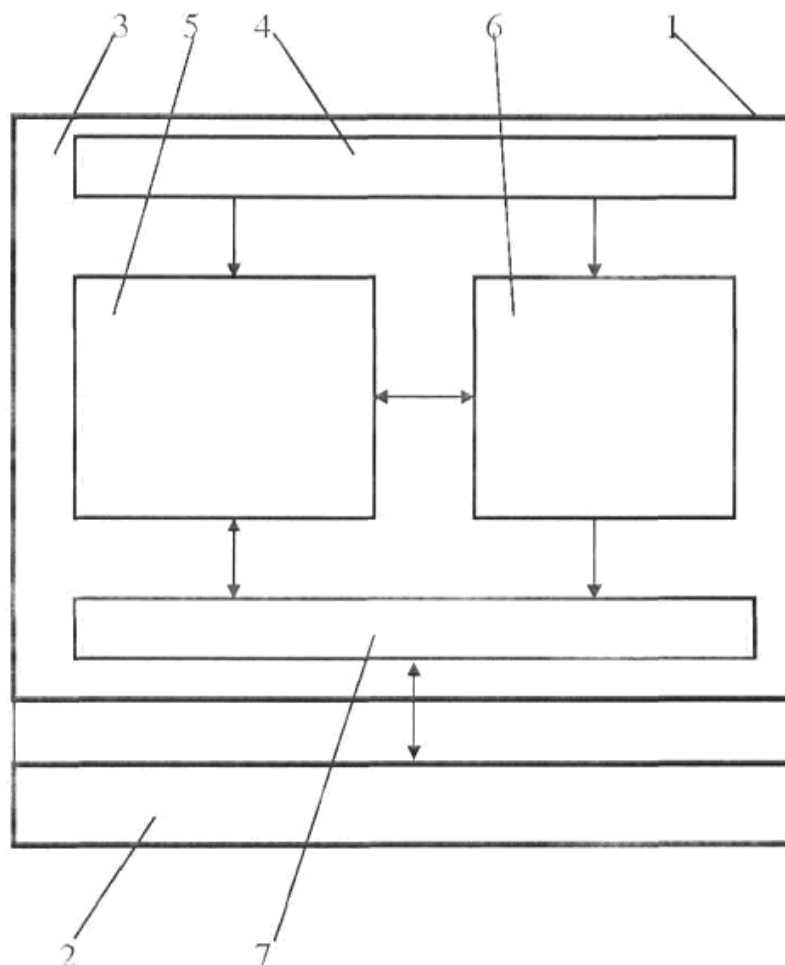
В режимі захисту від імітації даних ключ виконує авторизацію, аналогічну процедурі, описаній в попередньому пункті. Але додатково використовується процедура вироблення імітовставки. Імітовставка дозволяє на приймальному боці перевірити, що дані не були змінені під час передачі по каналу зв'язку. Ідея цього методу полягає в тому, що за допомогою складної односторонньої функції, результат якої залежить від переданих даних, виробляється імітовставка — коротке додаткове повідомлення. Приймальна сторона проводить аналогічну операцію з прийнятими даними і звіряє обчислене значення імітовставки з прийнятим. Якщо вони співпадають, дані вважаються дійсними, якщо ж ні — це признак спроби проведення атаки. Для зловмисника велику складність представляє перетворити повідомлення таким чином, щоб імітовставка залишилася такою ж, як і в початковому повідомленні. А не знаючи ключа, за допомогою якого це здійснюється, задача стає нерозв'язною в розумних часових рамках. Так само не знаючи ключа неможливо виробити правильну імітовставку для спотвореного повідомлення.

3. Робота в режимі шифрування даних.

- Режим роботи з шифруванням даних дозволяє крім забезпечення надійності переданих даних ще й можливість сховати ці дані від прослуховування зломисником, який підключений до каналу зв'язку і має можливість перехоплювати весь процес обміну даними. Особливістю цього режиму є уникнення повторів блоків даних навіть при передачі однакової інформації (це так званий режим гамування). Такий метод ускладнює аналіз зашифрованого потоку даних і обмежує можливість визначити передані дані в розумних часових рамках.

#### ФОРМУЛА КОРИСНОЇ МОДЕЛІ

- 10 1. Пристрій ідентифікації користувача та захисту від реверс-інжинірингу, що містить корпус, в якому розміщено мікроконтролер з програмними блоками, порт USB, який **відрізняється** тим, що блок захисту пам'яті мікроконтролера з'єднаний для обміну даними з блоками алгоритму захисту інформації і енергонезалежної пам'яті, які в свою чергу з'єднані для обміну даними з програмним драйвером, сумісним з USB.
- 15 2. Пристрій за п. 1, який **відрізняється** тим, що він інтегрований з програмним забезпеченням "Корпорація 2".



Комп'ютерна верстка С. Чулій

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