



УКРАЇНА

(19) **UA** (11) **107302** (13) **C2**  
(51) МПК  
**H04L 9/32** (2006.01)  
**G06K 9/18** (2006.01)

ДЕРЖАВНА СЛУЖБА  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ  
УКРАЇНИ

**(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД**

<b>(21)</b> Номер заявки:	<b>а 2013 14825</b>	<b>(72)</b> Винахідник(и):	<b>Яундалдерс Айгарс (LV)</b>
<b>(22)</b> Дата подання заявки:	<b>02.10.2012</b>	<b>(73)</b> Власник(и):	<b>РЕЛАТІВЕ ЦЦ, СІА,</b> Elizabetes iela 75, LV-1050 Riga, Latvija (LV)
<b>(24)</b> Дата, з якої є чинними права на винахід:	<b>10.12.2014</b>	<b>(74)</b> Представник:	<b>Сікачин Костянтин Володимирович,</b> реєстр. №292
<b>(31)</b> Номер попередньої заявки відповідно до Паризької конвенції:	<b>P-11-134</b>	<b>(56)</b> Перелік документів, взятих до уваги експертизою:	WO 2009/101549 A2, 20.08.2009 US 2009/0241175 A, 24.09.2009 US 2010/0070759 A1, 18.03.2010
<b>(32)</b> Дата подання попередньої заявки відповідно до Паризької конвенції:	<b>04.10.2011</b>		
<b>(33)</b> Код держави-учасниці Паризької конвенції, до якої подано попередню заявку:	<b>LV</b>		
<b>(41)</b> Публікація відомостей про заявку:	<b>25.02.2014, Бюл.№ 4</b>		
<b>(46)</b> Публікація відомостей про видачу патенту:	<b>10.12.2014, Бюл.№ 23</b>		
<b>(86)</b> Номер та дата подання міжнародної заявки, поданої відповідно до Договору РСТ	<b>PCT/LV2012/000015,</b> <b>02.10.2012</b>		

**(54) СПОСІБ ВИЗНАЧЕННЯ ІДЕНТИФІКАТОРА КОРИСТУВАЧА**

**(57)** Реферат:

Винахід стосується захисту інформації в комп'ютерних мережах і системах. Розроблений спосіб для визначення ідентифікатора користувача характеризується тим, що користувач підтверджує свій ідентифікатор за допомогою свого мобільного пристрою, його камери і спеціального прикладного програмного забезпечення, роблячи знімок і шляхом цифрової обробки реконструйованої графічно структурованої інформації провайдера послуг.

UA 107302 C2



Винахід стосується захисту інформації у комп'ютерних мережах і системах.

Існує спосіб автентифікації користувача з використанням паролів, де як пароліні фрагменти використовують заздалегідь визначене кольорове зображення [1].

Існує спосіб ідентифікації користувача з використанням PIN-коду, в якому користувачеві присвоюється унікальний персональний код для доступу до інформаційних систем [2].

Існує спосіб введення паролю для доступу до комп'ютерних баз даних з використанням динамічних зображень, генерованих комп'ютером [3].

Існує спосіб для доступу до захищених послуг з одноразовим введенням паролю [4].

Існують способи ідентифікації користувача з використанням імен користувача і паролів [5-8].

Існують способи ідентифікації користувача, які доповнюють введення імені користувача і паролю додатковими факторами автентифікації (багатофакторною автентифікацією) - генераторами одноразових паролів, друкованими кодовими картками, біометричними елементами та іншими факторами [9].

З метою зниження ризиків для безпеки, всі існуючі способи та системи вимагають від користувачів використання складних паролів, які важко запам'ятати, і які є незручними у використанні. Випадки втручання у системи провайдерів послуг з метою викрадення ідентифікаційних даних користувачів постійно зростають. Кожен додатковий фактор автентифікації, яким доповнюють імена користувачів і паролі, тягне за собою значні витрати і ускладнює досвід користувача, зводячи нанівець очікуване покращення безпеки.

Цей винахід має на меті розробити спосіб перевірки автентичності користувача, який би забезпечував надійну перевірку ідентичності, за допомогою мобільного пристрою, наприклад, телефону, без використання імені користувача і пароля.

Ця мета досягається шляхом запису користувачем на свій мобільний пристрій спеціально створеного реєстраційного зображення користувача, наприклад штрих-коду або QR-коду, яке відображається провайдером послуг, при цьому мобільний пристрій послідовно трансформує дані, отримані від фотодатчика, у структуровані дані, отримуючи ідентифікатор провайдера послуг, ідентифікатор ресурсу точки доступу провайдера послуг і унікальний маркер доступу і/або інші дані, вбудовані в це зображення, підтверджує цифровим підписом унікальний маркер доступу і/або інші дані, вбудовані в це зображення, і передає у точку доступу провайдера послуг у супроводі зі своїм відкритим ключем/цифровим сертифікатом, які використовуються для підпису цього повідомлення. Провайдер послуг перевіряє цифровий підпис отриманого повідомлення і, в разі успіху, асоціює отриманий відкритий ключ/цифровий сертифікат із профілем, який створив користувач.

При повторному відвідуванні, користувач записує у свій мобільний пристрій спеціально створене реєстраційне зображення, наприклад штрих-код або QR-код, яке відображається провайдером послуг. Це зображення, записане фотодатчиком, послідовно трансформується у структуровані дані, отримуючи ідентифікатор провайдера послуг, ідентифікатор ресурсу точки доступу провайдера послуг і унікальний маркер доступу і/або інші дані, вбудовані в це зображення. Користувач вибирає той же самий ідентифікатор, який він використовував під час реєстрації у цього провайдера послуг, мобільний пристрій підтверджує цифровим підписом унікальний маркер доступу і/або інші дані, вбудовані у реєстраційне зображення, і передає у точку доступу провайдера послуг у супроводі зі своїм відкритим ключем/цифровим сертифікатом, які використовуються для підпису цього повідомлення. Провайдер послуг перевіряє цифровий підпис отриманого повідомлення, зіставляє профіль користувача за допомогою відкритого ключа/цифрового підпису, які були збережені під час реєстрації, і дозволяє сеанс користувача відповідно до отриманого унікального маркера доступу або інших даних, вбудованих у реєстраційне зображення.

Для того, щоб почати користуватися системою певного провайдера послуг, наприклад, електронною поштою, форумами, сервісом електронної торгівлі, сервісом інтерактивного телебачення, тощо, більшість з яких доступні в режимі "онлайн", користувач відкриває сторінку ресурсу цього сервісу з комп'ютера або будь-якого іншого пристрою. Користувач створює профіль у цього провайдера послуг, вказавши будь-яку інформацію, яку провайдер послуг запитує спеціально для надання конкретної послуги. Якщо користувач вже створив профіль у певного провайдера послуг, користувач проходить автентифікацію відповідно до цього профілю за допомогою будь-яких засобів автентифікації, які він міг використовувати під час створення профілю. Користувач записує спеціально створене реєстраційне зображення, наприклад штрих-код або QR-код, за допомогою прикладного програмного додатку на даному мобільному пристрої, наприклад, смартфоні. Прикладний програмний додаток послідовно трансформує дані, отримані від фотодатчика, у структуровані дані, отримуючи ідентифікатор провайдера послуг, ідентифікатор ресурсу точки доступу провайдера послуг і унікальний маркер доступу

і/або інші дані, вбудовані в це зображення. Мобільний пристрій підтверджує цифровим підписом унікальний маркер доступу і/або інші дані, вбудовані в це зображення, і передає у точку доступу провайдера послуг у супроводі зі своїм відкритим ключем/цифровим сертифікатом, які використовуються для підпису цього повідомлення. Провайдер послуг перевіряє цифровий підпис отриманого повідомлення і, в разі успіху, асоціює отриманий відкритий ключ/цифровий сертифікат із профілем, який створив користувач.

У тих випадках, коли додаткові перевірки безпеки потрібні, щоб почати користуватися деякими послугами, наприклад, банківськими послугами, від користувачів можуть вимагати особистого відвідування приміщення провайдера послуг. Провайдер послуг може, таким чином, надати особисто користувачу реєстраційне зображення, наприклад, роздрукувавши його у реєстраційній формі на отримання послуги, показуючи на екрані комп'ютера, тощо. Користувач записує, таким чином, це реєстраційне зображення за допомогою прикладного програмного додатку на своєму мобільному пристрої і виконує наступні етапи реєстрації, як описано вище.

При повторному відвідуванні, користувач записує у свій мобільний пристрій спеціально створене реєстраційне зображення, наприклад штрих-код або QR-код, яке відображається провайдером послуг. Це зображення, записане фотодатчиком, послідовно трансформується у структуровані дані, отримуючи ідентифікатор провайдера послуг, ідентифікатор ресурсу точки доступу провайдера послуг і унікальний маркер доступу і/або інші дані, вбудовані в це зображення. Користувач вибирає той же самий ідентифікатор, який він використовував під час реєстрації у цього провайдера послуг, мобільний пристрій підтверджує цифровим підписом унікальний маркер доступу і/або інші дані, вбудовані у реєстраційне зображення, і передає у точку доступу провайдера послуг у супроводі зі своїм відкритим ключем/цифровим сертифікатом, які використовуються для підпису цього повідомлення. Провайдер послуг перевіряє цифровий підпис отриманого повідомлення, зіставляє профіль користувача за допомогою відкритого ключа/цифрового підпису, які були збережені під час реєстрації, і дозволяє сеанс користувача відповідно до отриманого унікального маркера доступу або інших даних, вбудованих у реєстраційне зображення. На цьому процес автентифікації користувача завершується.

У тих випадках, коли провайдер послуг потребує виконання додаткових заходів з контролю безпеки під час процесу реєстрації, провайдер послуг може зареєструвати IP-адресу вихідного мобільного пристрою, що використовується для надсилання повідомлення запиту про реєстрацію, і встановити обмеження щодо географічного положення для наступної дозволеної сесії користувача. Наприклад, провайдер послуг може дозволити доступ до сесії користувача тільки з пристроїв, які знаходяться в безпосередній близькості до IP-адреси вихідного мобільного пристрою, що ускладнює запуск будь-яких атак з викрадення ідентифікаційних даних.

Спосіб і система для визначення ідентифікатора користувача, описані тут, забезпечують надійний процес автентифікації користувача за допомогою мобільного пристрою, наприклад телефону. Спосіб може використовуватися для будь-якого сайту ресурсів провайдера послуг, не обмежуючись веб-сайтом в мережі Інтернет, доступ до якого здійснюється з персонального комп'ютера. Єдиною технологічною передумовою для такого сайту ресурсів є здатність відображати динамічно генероване облікове/реєстраційне зображення. Спосіб може бути реалізований для будь-якої операційної системи, браузера або програмного забезпечення прикладного програмного інтерфейсу (API).

Посилання:

1. Патент RU 2348974, C2, G06K9/00, 2008.
2. Патент RU 2385233, C1, B42D15/10, 2008.
3. Патент RU 2263341, C1, G06F1/00, 2005.
4. Патент RU 2308755, C2, G06F17/00, 2005.
5. Патентна заявка US 2008/0120717, A1, G06F21/00, 2008.
6. Патентна заявка US 2009/0307182, A1, G06N5/02, 2009.
7. Патентна заявка US 2009/0228370, A1, G06Q30/00, 2009.
8. Патентна заявка WO 2008/151209, A1, H04K1/00, 2006.
9. Патент RU 2382408, C2, G06K9/00, 2008.

## ФОРМУЛА ВИНАХОДУ

- Спосіб визначення ідентифікатора користувача, який включає: створення нового профілю користувача або автентифікації відповідно до існуючого профілю користувача за допомогою вже існуючих засобів автентифікації, який **відрізняється** тим, що:
- профіль користувача створюють з реєстрацією IP-адреси мобільного пристрою, що використовується для надсилання повідомлення про реєстрацію, та встановлюють можливість географічного обмеження для наступної дозволеної сесії користувача за IP-адресою, після створення профілю користувача, користувач записує реєстраційне зображення за допомогою прикладного програмного додатку на даному мобільному пристрої;
- прикладний програмний додаток послідовно трансформує дані з фотодатчика у структуровані дані, отримуючи ідентифікатор провайдера послуг, ідентифікатор ресурсу точки доступу провайдера послуг і унікальний маркер доступу, вбудований в це зображення;
- мобільний пристрій підтверджує цифровим ідентифікатором пристрою унікальний маркер доступу, вбудований в це зображення, і передає у точку доступу провайдера послуг у супроводі зі своїм відкритим ключем/цифровим сертифікатом, які використовуються для підпису цього повідомлення;
- провайдер послуг перевіряє цифровий ідентифікатор пристрою отриманого повідомлення і, в разі успіху, асоціює отриманий відкритий ключ/цифровий сертифікат із профілем, який створив користувач;
- при повторному відвідуванні, користувач записує у свій мобільний пристрій спеціально створене реєстраційне зображення, яке відображається провайдером послуг; це зображення, записане фотодатчиком, послідовно трансформується у структуровані дані, отримуючи ідентифікатор провайдера послуг, ідентифікатор ресурсу точки доступу провайдера послуг і унікальний маркер доступу, вбудовані в це зображення;
- користувач вибирає той же самий ідентифікатор, який він використовував під час реєстрації у цього провайдера послуг, мобільний пристрій підтверджує цифровим ідентифікатором пристрою унікальний маркер доступу, вбудований у реєстраційне зображення, і передає у точку доступу провайдера послуг у супроводі зі своїм відкритим ключем/цифровим сертифікатом, які використовуються для підпису цього повідомлення;
- провайдер послуг перевіряє IP-адресу вихідного мобільного пристрою, цифровий ідентифікатор пристрою отриманого повідомлення, зіставляє профіль користувача за допомогою відкритого ключа/цифрового підпису, які були збережені під час реєстрації, і дозволяє сеанс користувача відповідно до отриманого унікального маркера доступу, вбудованого у реєстраційне зображення; на цьому процес автентифікації користувача завершується.

---

Комп'ютерна верстка Л. Литвиненко

---

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