УДК 336.717.13.004.738.5

О.В. Клювак

Особливості технологій аутентифікації в Інтернет-платіжних системах на основі банківських карток

Розглянуті основні типи та методи аутентифікації, які застосовуються під час здійснення Інтернет-транзакцій. Акцентовано увагу на недоліках у наявних технологіях аутентифікації та визначені основні критерії побудови удосконаленого протоколу аутентифікації як засобу подолання зазначених недоліків у Інтернет-платіжних системах на основі банківських карток.
Ключові слова: аутентифікація, електронно-цифровий підпис (ЕЦП), цифровий сертифікат, інфраструктура відкритих ключів (PKI), хеш-функція (алгоритм), смарт-карти.

Для забезпечення недоторканості та захисту даних в електронних платіжних системах важливим є знати точно, з ким мають справу учасники Інтернет-транзакцій, а також упевненість у тому, що отримані дані є справжніми. Аутентифікація допомагає встановити надійні відносини між сторонами, які беруть участь у всіх типах транзакцій, дозволяючи виявляти усі зловживання [1]. Проте у механізмі аутентифікації під час здійснення Інтернет-транзакцій спостерігаються деякі недоліки та резонним є виокремлення основних критеріїв до протоколів аутентифікації, які на сьогодні здатні забезпечити достатній рівень безпеки розрахунків.

Питання особливостей аутентифікації в електронній комерції широко розглядають та досліджують як науковці, так і фахівці банківської справи. Зокрема, В. Степаненко, начальник управління інформаційних та банківських технологій Асоціації українських банків, акцентує увагу у своїх дослідженнях на електронно-цифровому підписі, а саме – на проблемах та перспективах його розвитку, використанні ЕЦП у банківській системі [2]. Автор Дж. Вакка у своїй книзі «Секреты безопасности в Internet» чітко аналізує наявні методи аутентифікації учасників електронних розрахунків [3]. Науковці А. Сарбуков та А. Грушо наводять чітку класифікацію методів аутентифікації, розкривають суть протоколу аутентифікації [5]. Дослідники В. Яковина та О. Одуха пропонують покращений протокол взаємної аутентифікації з використанням смарт-карт [6].

Цілями статті є розглянути основні типи та методи аутентифікації, які застосовуються під час здійснення Інтернет-транзакцій; проаналізувати основні недоліки в наявних технологіях аутентифікації та запропонувати основні критерії до побудови удосконаленого протоколу аутентифікації в Інтернет-платіжній системі на основі банківських карток, як засобу подолання цих недоліків.

Методи аутентифікації покликані захищати автоматизовану систему інформації шляхом управління доступом до ресурсів системи обробки даних. Ці методи дають змогу визначити істинність ідентифікаторів апаратних засобів та інформації для передачі, а також учасників транзакцій, зокрема в електронній комерції – покупця (власника платіжної картки), продавця та платіжного шлюзу [3, с. 119-130].

На рис. 1 зображуються можливі варіанти двосторонніх відносин покупців та продавців в електронній комерції. Тип двосторонніх відносини у першому варіанті є досить незручним для користувачів, адже потребує персональної ідентифікації та аутентифікації у кожного продавця. Другий тип передбачає одноразову аутентифікацію покупця для багатьох продавців за наявності їхньої спільної згоди. При третьому типові покупці та продавці покладаються на провайдера послуг аутентифікації, що повністю виключає процедуру

взаємної двосторонньої аутентифікації між покупцем і продавцем. Цей спосіб аутентифікації називається циклом довір'я, він дозволяє включати у процедуру взаємодії покупця та продавця третю особу, наприклад, банк. І, останній тип розвитку аутентифікації в мережі пов'язаний із взаємодією багатьох серверів із надання послуг аутентифікації між собою. Такий спосіб сервісу називається «федеральною службою мережевої аутентифікації» (рис. 1).

Усі випадки мережевої аутентифікації зводяться до двосторонньої аутентифікації на рівні протоколів аутентифікації між компонентами автоматизованих систем. Причому поява постійного пароля в мережевому трафіку знижує безпеку мережевої аутентифікації. Тому у мережевій аутентифікації необхідно використовувати одноразові паролі або аутентифікацію за допомогою апаратних засобів (рис. 2).

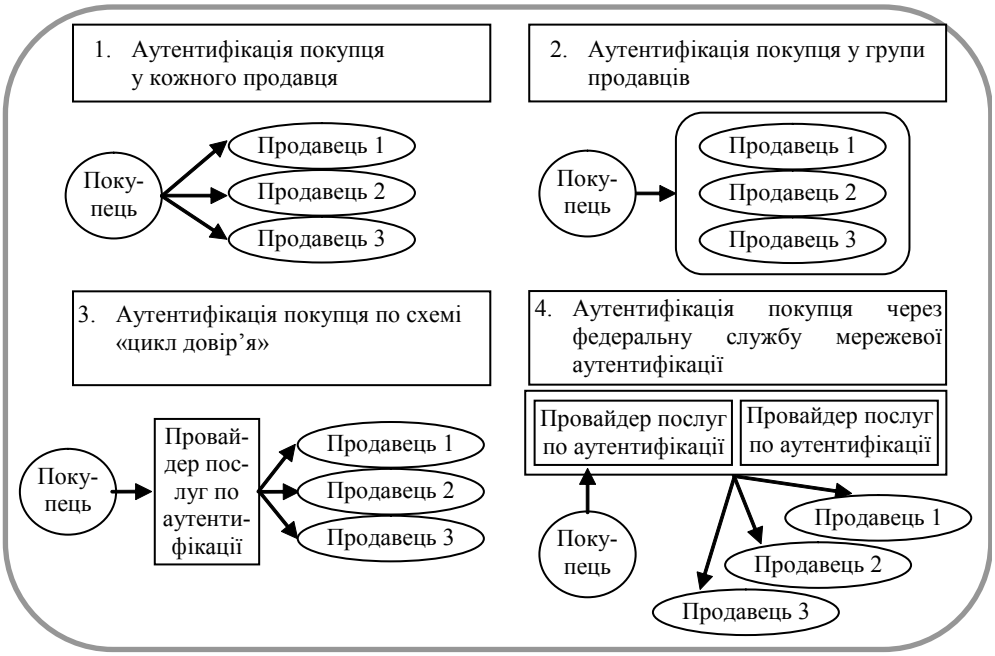

Рис.1 Варіанти двосторонніх відносин покупців та продавці в електронній комерції

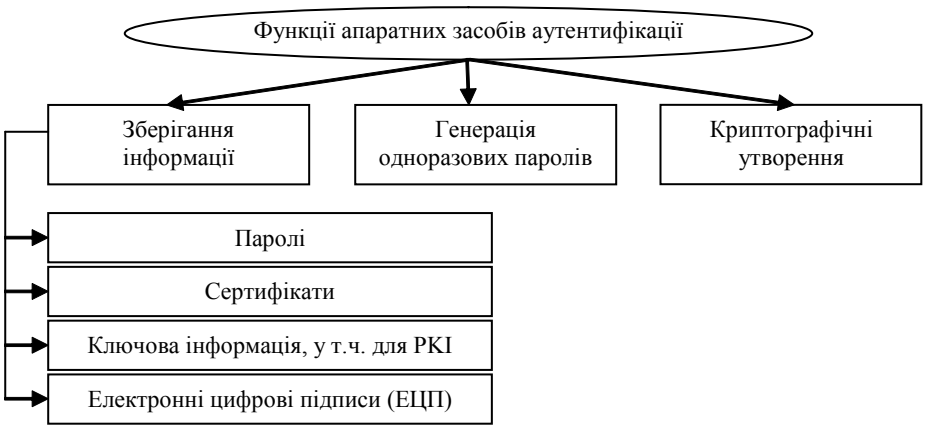

Рис. 2 Функції, які реалізуються за допомогою апаратних засобів аутентифікації (смарт-карти, USB-ключі, Touch-Memory)

У таблиці 1 описані аутентифікації за допомогою апаратних засобів та електронно-цифрових підписів (табл. 1) [4].

Не менш поширеною технологією аутентифікації в електронній комерції вважається технологія аутентифікації за допомогою одноразових паролів (рис. 3). Протокол аутентифікації у системі одноразових паролів полягає у наступному:

– клієнт надсилає серверу пакети ініціалізації;
– сервер відправляє клієнту порядковий номер та випадкове число;
– клієнт вводить пароль.

Пароль з'єднується з випадковим числом та порядковим номером. Вихідна функція переводить бітове число у читабельну форму, і це число використовується як одноразовий пароль. Перевірка одноразового пароля здійснюється після його створення на сервері. Для перевірки пароля система пропускає отриманий одноразовий пароль через хеш-функцію. Якщо результат цієї операції співпадає з попереднім паролем, то результат аутентифікації вважається позитивним і новий пароль зберігається для подальшого використання. Протокол аутентифікації у системі одноразових паролів заснований на технології клієнт-сервер. Клієнтом сервера зазвичай є сервер мережевого доступу. Сервери отримують запити від користувачів на підключення, проводять аутентифікацію цих користувачів, формують, а потім відправляють на сервер мережевого доступу всю конфігураційну інформацію, яка необхідна клієнту для обслуговування користувача. Двосторонній зв'язок клієнта

Таблиця 1

Особливості аутентифікацій за допомогою апаратних засобів та електронно-цифрових підписів (ЕЦП)

Типи аутентифікацій	Особливості типів аутентифікацій
1. Аутентифікація за допомогою апаратних засобів:	
1.1 За схемою запит-відповідь	Власник картки підключається до сервера аутентифікації та передає йому PIN або User ID. Сервер передає покупцеві випадкове число, яке надсилається на підключену до пристрою покупця інтелектуальну карту. Карта шифрує отримане число та передає результат серверу. Сервер також шифрує надіслане ним випадкове число, використовуючи ключ власника картки. Порівняння шифротексту, отриманого від покупця, та шифротексту, обчисленого на сервері, дозволяє аутентифікувати покупця.
1.2. За схемою антентифікації із синхронізацією	У схемі із синхронізацією за часом на апаратному пристрої покупця (інтелектуальній карті) і на сервері працює секретний алгоритм, який синхронно створює паролі та замінює старі паролі на нові. При аутентифікації власник картки вводить свій PIN або User ID і встановлює у рідері персональну інтелектуальну карту. Порівняння паролю, зчитаного з карти, з отриманим на сервері, дозволяє аутентифікувати покупця.
2. Аутентифікація за допомогою ЕЦП	ЕЦП може використовуватися як засіб аутентифікації, якщо він розміщений на апаратних засобах типу інтелектуальної карти. Карта надає серверу підписаний ЕЦП ідентифікатор або PIN покупця, сервер перевіряє ЕЦП і тим самим здійснює аутентифікацію покупця. Така аутентифікація можлива у разі обмеженої кількості покупців, що дозволяє зберігати на сервері інформацію про ЕЦП усіх покупців. Якщо покупців дуже багато, то підпис покупця повинен містити сертифікат відповідно до стандарту X.509. для безпечного управління ключами у середовищі великої кількості покупців або систем необхідна інфраструктура відкритих ключів (PKI).

та сервера реалізується у зашифрованому вигляді, що виключає компрометацію користувацької інформації. Для попарної аутентифікації «клієнт-сервер», «клієнт-користувач» можуть використовуватися різні протоколи прикладного, канального або мережевого рівнів.

При аутентифікації за допомогою однонаправлених функцій на сервері, який перевіряє правильність введеного користувачем (першим учасником протоколу) паролю, зовсім не обов'язково зберігати паролі користувачів. Достатньо навчити сервер відрізняти правильні паролі від неправильних. Тоді на сервері будуть присутні не самі паролі, а їх хеш-значення:

1. Перший учасник протоколу надсилає на сервер свій пароль.
2. За допомогою однонаправленої функції сервер обчислює хеш-значення для надісланого паролю.
3. Сервер порівнює обчислене хеш-значення з еталоном, який зберігається у його пам'яті, і відповідно робить висновок щодо правильності пароля.

Оскільки при такій схемі аутентифікації користувачів немає потреби зберігати паролі на сервері, тож і хвилюватися за те, що відбудеться злам захисту сервера і викрадення файла з паролями, немає підстав. Список хеш-значень, які відповідають паролям зареєстрованих користувачів, абсолютно не є суттєвим для зловмисника, бо знайти пароль за його хеш-значенням шляхом перетворення однонаправленої функції йому не вдасться. Файл із хеш-значеннями, отриманими з паролів, може підлягати словниковій атаці. Склавши словник приблизно з одного мільйона найпоширеніших паролів, зловмисник застосовує до них хеш-функцію. В результаті він отримає файл об'ємом до десяти мегабайт. Далі зловмисник викрадає із сервера файл із паролями, зашифрованими за допомогою хеш-функцій, і порівнює із своїм файлом, який містить хеш-значення для паролів, які часто використовуються. Хеш-значення, які співпали, дозволять зловмисникові визначити деякі паролі. Протистояти словниковій атаці частково можна введенням у схему аутентифікації зареєстрованих користувачів, так званих «***родзинок***». «Родзинка» являє собою випадковий бітовий рядок, який приєднується до пароля перш ніж до нього буде застосована хеш-функція. Згодом на сервері запам'ятовується як обчислена хеш-функція, так і відповідна йому «родзинка». Якщо кількість можливих «родзинок» достатньо велика, то словникова атака є беззмістовною. Зловмисник змушений обчислювати хеш-значення не тільки для кожного пароля, але й для кожної «родзинки». Зміст введення «родзинок» у схему аутентифікації користувачів полягає у тому, щоб змусити зловмисника здійснювати пробне шифрування усіх паролів, які входять у створений ним словник, кожного разу, коли він намагається розкрити який-небудь окремий пароль, замість того, щоб наперед вирахувати хеш-значення цих паролів, а згодом просто порівнювати отриманні значення з еталонними, викраденими із сервера.

Проте «родзинок» потрібно багато. І така схема аутентифікації не може служити панацеєю. Вона забезпечує захист лише від словникової атаки всього файла з паролями, зашифрованими за допомогою однонаправленої функції. Але така схема є безсилою, коли потужній атаці підлягає окремий пароль конкретного користувача.

Навіть за наявності «родзинок» схема аутентифікації користувачів шляхом перевірки їх паролів має дуже важливий недолік. Адже не виключено, що лінія зв'язку, яка з'єднує персональний комп'ютер користувача із сервером інформаційно-комерційної служби, проходить територіями 33-х країн, законодавство яких по-різному трактує права своїх та іноземних громадян на збереження таємниці особистого листування. Саме тому дізнатися пароль користувача в принципі може той, хто зуміє підключитися до цієї лінії зв'язку або звернутися до пам'яті сервера і дізнатися пароля до того, як для нього буде обчислено

відповідну хеш-функцію. Щоб зменшити ризики компрометації пароля, його необхідно періодично змінювати. Це здійснюється наступним чином:

Користувач генерує випадкове число R і надсилає його серверу, котрий обчислює, виходячи з цього числа та однонаправленої функції f значення $x_1 = f(R), x_2 = f(f(R)), x_3 = f(f(f(R)))$ і т.д. 101 раз. Перших 100 обчислених значень x_1, x_2, x_3, x_{100} передаються користувачеві як список паролів, який він повинен зберігати у таємниці. А x_{101} зберігається на сервері.

Якщо користувач захоче зареєструватися для роботи на сервері, йому достатньо буде ввести своє ім'я та число x_{100}. Сервер обчислює $f(x_{100})$ і порівнює його з x_{101}. У випадку співпадіння користувачеві буде дозволений доступ до сервера, котрий згодом замінює x_{101} на x_{100}. А користувач викреслює x_{101} із свого списку паролів. Наступного разу, коли користувач знову захоче отримати доступ до сервера, він знайде у списку паролів наступне за порядком незакреслене значення x_j. Сервер обчислює $f(x_j)$ і порівнює із збереженим x_{j+1}.

Зловмисник, котрий проникнув на сервер, не зможе дізнатися наступний пароль користувача x_j за значенням x_{j+1}, який зберігається на сервері, оскільки функція f є однонаправленою. З цієї ж причини, навіть якщо зловмисник перехопить x_j, то це дозволить йому зареєструватися під іменем користувача лише один раз. А значення x_1, x_2, x_3, x_{j-1} так і залишаться для зловмисника таємницею за умови надійного зберігання їх власником.

Проте ні «родзинки», ні періодична зміна пароля не гарантують достатньо високого рівня захисту від перехоплення всіх повідомлень, котрі надсилаються користувачем по лінії зв'язку, яка з'єднує його із сервером.

Вирішити цю проблему допомагає застосування криптографії з відкритим ключем.

Припускається, що на сервері знаходиться файл, у якому зберігаються відкриті ключі всіх користувачів. Криптографічний протокол, котрий дозволяє здійснювати аутентифікацію користувачів, виглядає так:

1. Сервер генерує випадковий рядок і надсилає його користувачеві.
2. Користувач шифрує цей рядок за допомогою свого таємного ключа і надсилає назад на сервер.
3. На сервері здійснюється розшифрування повідомлення, яке надійшло від користувача, за допомогою його відкритого ключа.
4. Якщо отриманий у результаті відкритий текст ідентичний випадковому рядку, раніше надісланому користувачеві, останній отримує доступ до сервера.

Оскільки тільки користувач знає свій таємний ключ, то ніхто не може видати себе за нього. Цей таємний ключ являє собою довгий бітовий рядок, який важко відтворити по пам'яті, і тому у розпорядженні користувача повинен бути інтелектуальний термінал, надійно захищений від зламу і здатний автоматично здійснювати набір потрібного таємного ключа при шифруванні повідомлень. Проте, незважаючи на додаткову умову, найважливішим є те, що таємний ключ не потрібно передавати на сервер.

Звичайно, що з боку користувача немає змісту шифрувати на своєму таємному ключі випадкову бітову послідовність. Тому на практиці для аутентифікації користувачів зазвичай використовується складніший криптографічний протокол:

1. Користувач здійснює деякі спеціальні обчислення на основі попередньо згенерованої ним випадкової бітової послідовності і свого таємного ключа. Згодом він надсилає обчисленні ним значення на сервер.
2. Сервер надсилає користувачеві випадкову бітову послідовність, яка відрізняється від тієї, яка була задіяна користувачем.

3. Користувач здійснює спеціальні обчислення на основі двох випадкових бітових послідовностей та свого таємного ключа. Обчисленні значення надсилаються на сервер.
4. На сервері здійснюються деякі спеціальні обчислення на основі надісланих користувачем значень та відкритого ключа, щоб переконатися у тому, що він дійсно є власником таємного ключа.
5. Якщо перевірка дає позитивний результат, користувачеві надається доступ до сервера.

Якщо користувач, своєю чергою, не довіряє серверу, він може вимагати, щоб сервер аналогічним чином посвідчив свою особу, користуючись тим самим протоколом [4].

Надійність технології з відкритим ключем базується на математично доведеному факті практичної неможливості обчислення секретного ключа з використанням сучасних обчислювальних засобів за невеликий період часу. Пропоновані сьогодні криптосистеми з відкритим ключем опираються на один із таких типів необоротних перетворень:

– розклад великих чисел на прості множники;
– обчислення логарифму в кінцевому полі;
– обчислення коренів алгебраїчних рівнянь [5].

Отже, традиційно аутентифікація учасників розрахунків в Інтернеті базується на наданні певного ідентифікатора та відповідного пароля у платіжній системі. Надалі система порівнює отримані дані з даними, що зберігаються у файлі паролів. Оскільки паролі зберігаються у вигляді відкритого тексту, такий підхід, очевидно, є вразливим до викрадення пароля. Для того, щоб позбутися атаки на відкритий файл паролів, було запропоновано перетворити файл паролів на таблицю верифікації. Така таблиця містить значення односторонньої хеш-функції від паролів користувачів. Така схема забезпечує захист паролів навіть у випадку викрадення таблиці верифікації. Однак наявність таблиці верифікації залишає можливою модифікацію даних, атаку на основі бази значень хешу та збільшує вартість захисту та супроводу таблиці. Відтак були запропоновані схеми, що не використовували таблиць верифікації. У таких схемах поширені мітки часу чи порядкові номери для протидії атакам повтором. На жаль, донедавна більшість таких схем забезпечувала тільки односторонню аутентифікацію, тоді як на сучасному етапі розвитку комунікаційних технологій та Інтернету вимагаються двосторонні схеми аутентифікації (як користувача, так і сервера). Крім того, перевагу мають протоколи аутентифікації, що одночасно забезпечують обмін сеансовими ключами шифрування.

Завдяки своїй низькій вартості, компактності та криптографічним можливостям, смарт-карти знайшли широке застосування у багатьох додатках електронної комерції, протоколах мережевої безпеки та схемах віддаленої аутентифікації. Тому, на нашу думку, протоколи аутентифікації з використанням технології смарт-карти у Інтернет-платіжних системах на основі банківських карток повинні враховувати такі критерії:

– відсутність таблиць верифікації: на сервері не слід зберігати жодних таблиць паролів чи верифікації;
– вільний вибір пароля: користувачі можуть вільно вибирати свої власні паролі;
– низьке комунікаційне та обчислювальне навантаження: завдяки обмеженням обчислювальної потужності смарт-карт вони можуть не забезпечити високих обчислювальних можливостей при широкій смузі пропускання;
– взаємна аутентифікація: користувачі і сервери повинні взаємно аутентифікувати один одного.

Отже, при побудові протоколів аутентифікації в Інтернет-платіжних системах на основі банківських пластикових карток необхідно здійснювати якісний криптоаналіз, який надав би можливість прослідковувати стійкість цього протоколу до таких можливих атак:

– підбір пароля;
– атака з компрометацією ключа;
– використання сценарію зв'язаних ключів;
– колізії в хеш-функціях [6].

Список використаних джерел

1. Решение проблем безопасности для электронной коммерции [Электронный ресурс]. – Режим доступа: kek.ksu.ru/EOS/ITE/notes/ec6.rtf.
2. Степаненко В. Электронная цифровая подпись Текущее состояние, проблемы, перспективы развития [Электронный ресурс] / В. Степаненко. – Режим доступа: http://www.sib.com.ua/arhiv_2006/2006-6/2006_6_ podpis'.html.
3. Вакка Дж. Секреты безопастности в Internet / Дж. Вакка. – К. : Диалектика, 1997. – 512 с., ил.
4. Иллюстрированный самоучитель по защите информации. Формальный анализ криптографических протоколов [Электронный ресурс]. – Режим доступа: http://www.svit-it.com.ua/kb/pi/7/Index6.htm.
5. Сарбуков А. Аутентификация в компьютерных системах [Электронный ресурс] / А. Сарбуков, А. Грушо. – Режим доступу: http://www.infosecurity.ru/_gazeta/content/040316/article1.html .
6. Яковина В. Вдосконалений протокол взаємної аутентифікації на основі смарткарт для побудови модуля захисту розподіленої системи теплового проектування [Электронный ресурс] / В. Яковина, О. Одуха. – Режим доступа: www.nbuv.gov.ua/portal/natural/VNULP/Komp-nauky/2009…/31. pdf.

Клювак О.В. Особенности технологий аутентификации в Интернет-платежных системах на основе банковских карточек.

Рассмотрены основные типы и методы аутентификации, которые применяются во время выполнения Интернет-транзакций. Акцентировано внимание на недостатках в существующих технологиях аутентификации и определены критерии построения усовершенствованного протоколf аутентификации как средства преодоления отмеченных недостатков в Интернет-платежных системах на основе банковских карточек.

Ключевые слова: аутентификация, электронно-цифровая подпись (ЭЦП), цифровой сертификат, инфраструктура открытых ключей (PKI), хеш-функция (алгоритм), смарт-карты.

Kliuvak O.V. Features of Authentification Technologies in the Internet Payment Systems on the Basis of Bank Cards.

Basic types and methods of authentification, which are used during the realization of Internet-transactions, are considered. Special attention is paid to failings in existing technologies of authentification. The basic criteria of construction of the improved authentification protocol as the mean of overcoming of the abovementioned failings in the Internet-payment systems based on bank cards are determined.

Key words: authentification, electronic digital signature (EDS), digital certificate, public key infrastructure (PKI), hashing-function (algorithm), Smartcards.

Надійшло 19.04.2010