УДК 004.056.55 **Ряба О.І., Черниш Л.Г., Каменщик Ю.О.**

ПРОВЕДЕННЯ ЕЛЕКТРОННИХ ПЛАТЕЖІВ ЗА ДОПОМОГОЮ «СЛІПОГО» ПІДПИСУ ЧАУМА НА БАЗІ КРИПТОСИСТЕМИ RSA

В статті розглянуто такий криптографічний метод захисту платіжних систем як «сліпий» підпис Чаума на базі криптосистеми RSA, описана оцінка його ефективності та надійності. Детально розглянуто та проаналізовано алгоритм його роботи. Наведено алгоритм забезпечення анонімності платежів.

Ключові слова**:** «сліпий» підпис, анонімність, електронні гроші, криптосистема RSA, платіжна система.

Вступ. Необхідність зниження витрат на управління готівковим грошовим обігом, загострення конкурентної боротьби за грошові ресурси між різними фінансовими інститутами в сукупності з подальшими успіхами в області інформаційних і фінансових технологій зумовили появу нового платіжного засобу – готівкових електронних грошей. Електронні платіжні системи (англ. Electronic Payment Systems) — це системи, призначені для здійснення платіжних операцій за допомогою електронних грошей у всесвітній мережі Інтернет. За допомогою платіжної системи можна здійснювати розрахунок за товари та послуги різних проектів і сервісів. Наприклад, оплачувати мобільний зв'язок, комунальні послуги, кабельне або супутникове телебачення, послуги Інтернет-провайдерів, а також різноманітні покупки в Інтернет- магазинах.

Аналіз останніх досліджень та постановка проблеми. Електронні гроші цілком копіюють реальні гроші [1]. При цьому емітент випускає електронні аналоги реальних грошей, надалі «монети». Далі вони купуються користувачами, які з їх допомогою оплачують придбані товари і послуги, після чого продавець погашає їх у емітента. *Актуальність* дослідження електронних платежів невпинно росте, оскільки вони мають дуже важливі і незаперечні переваги, такі як: доступність; простота використання; мобільність; оперативність; безпека.

Метою даної роботи є детальний огляд ефективності та надійності проведення електронних платежів за умовою використання «сліпого» підпису Чаума на базі протоколу RSA.

*Основна частина***.** Забезпечення анонімності в електронній готівці полягає в використанні «сліпого» цифрового підпису (blind signature), яку запропоновано Девідом Чаумом (David Chaum) [2, 3]. Алгоритми «сліпого» підпису можливо класифікувати наступним чином: класичний «сліпий» підпис; повністю «сліпий» підпис; «сліпий» підпис з використанням криптосистеми RSA; несподіваний «сліпий» підпис (на базі RSA); система Брандса; система Фергюсона.

Далі розглянемо більш детальніше систему «сліпого» підпису з використанням криптосистеми RSA.

Згідно цієї системи [4], підписувач інформації бачить її лише в частині йому необхідній, але своїм цифровим підписом завіряє достовірність всієї інформації: емітент бачить гідність купюр, але не знає їх серійних номерів, які знає тільки їх власник. Таким чином, покупець має електронні гроші, які мають визначену, підтверджену вартість.

Грошовим сертифікатом («монетою» номіналу i) у цій системі є наступні дані[3]:

$$Coin\ (i, X) = \{i, X, g_i^{-1}\ (f\ (X))\},$$

де X – обираний клієнтом випадковий серійний номер «монети», який є елементом великої множини $M' \subset M = (Z/mZ)^*$; m – складене число, чиє розкладання на множники відомо тільки банку; $f: M' \longrightarrow M$ – відображення,що легко обчислюється, публічно відоме і важко оборотне для всіх учасників платіжної системи, крім, можливо, банку; $g_i(x)=x^{E_i}: M \longrightarrow M$ – публічно відомі відображення з підходящими показниками ступеня.

Відображення g_i^{-1} є RSA-підписом банку, відповідної номіналу «монети» i. Якщо в системі використовується кілька валют, то кожній валюті повинен відповідати свій набір функцій g_i (індекс валюти ми опускаємо). Множина M (число m) і відображення f також можуть залежати від номіналу і валюти. Описані «монети» банк може виготовляти для клієнта наосліп. Покупець здійснює платіж, передаючи продавцю набір «монет», сума номіналів яких дорівнює величині платежу. Продавець відправляє отримані «монети» в банк для авторизації. Банк засвідчується в тому, що надані «монети» відсутні у списку використаних «монет», після чого заносить їх до цього списку, збільшує суму на рахунку продавця на величину платежу і повідомляє продавцеві про успіх. Платежі в даній системі абсолютно не пов'язані один з одним. Розглянемо деякі недоліки системи Чаума.

З теоретичної точки зору суттєвим недоліком системи Чаума є те, що платник і банк змушені довіряти один одному. Банк може присвоїти пред'явлену платником «монету», заявляючи, що вона вже була використана раніше. У свою чергу, шахрай може пред'являти претензії банку, заявляючи, що ніякого повторного використання монети не було, а банк просто хоче вкрасти її. Потрібна також довіру до продавця, якщо «монети» передаються йому у відкритому вигляді. Слід зазначити, що цей недолік не є специфічною властивістю «монет» Чаума, але висловлює фундаментальне властивість сертифікатів на пред'явника. Сертифікати на пред'явника не містять в собі ніякого секрету пред'явника, за допомогою якого він міг би доводити свої права на сертифікат. Таким чином, в системі Чаума можливі конфлікти, не розв'язані засобами самої системи. Це призводить до подорожчання платіжної системи, так як для обробки таких конфліктів потрібні особливі організаційні заходи (страхувальні фонди, чорні списки і т. п.).

Основною областю застосування платіжної системи є електронна комерція [5]. Для того щоб мати можливість вирішувати конфлікти в рамках торгової системи, будь-яка грошова транзакція повинна бути прив'язана до відповідної товарної транзакції таким чином, щоб платник мав можливість доводити факт оплати конкретного товару. Так як в рамках системи Чаума відсутня внутрішня можливість інтегрування з торговою системою, то це означає, що платник, крім гаманця (клієнта платіжної системи), повинен мати ще специфічного для даної торгової системи покупця (клієнта торгової системи), який буде пов'язувати грошові транзакції з товарними трансакціями. Рано чи пізно список використаних «монет» в платіжній системі Чаума перестане вміщатися у відведеному для нього сховищі. Крім того, час пошуку «монет» в цьому списку зростає із зростанням списку, хоча і логарифмічно. Тому, щоб мати можливість утримувати розмір списку в прийнятних межах, банк повинен обмежувати період оперативної платоспроможності «монет». У цьому випадку використані монети, платоспроможний період яких закінчився, можна видаляти зі списку. Занадто короткий період оперативної платоспроможності не додає платіжній системі споживчої привабливості. Тут потрібно відзначити, що швидкість росту розміру списку використаних «монет» тим вище, чим ширше діапазон і менше крок можливих платежів, так як для забезпечення широкого діапазону і малого кроку необхідно вводити багато номіналів монет. Як наслідок, зростає середня кількість «монет» в одному платежі. Збільшення середнього числа «монет» в одному платежі пропорційно збільшує час пошуку в списку використаних «монет».

Висновки. Постійний прогрес комп'ютерної техніки поступово знижує серйозність проблеми великого списку використаних «монет». Крім того, Чаум запропонував спосіб сліпого повернення банком здачі, що дозволяє використовувати для платежу всього лише одну «монету». Цікавими є майбутні перспективи розвитку «сліпого» підпису в бездротових мережах для тимчасової аутентифікації клієнта, в безкоштовних сервісах для розміщення файлів без реєстрації для передачі їх іншим користувачам з метою відслідкування скачувань по виданому гіперпосиланню.

ЛІТЕРАТУРА

1. С.В. Афоніна Электронные деньги, видання СПб: Питер, 2008. – с. 27.

2. Брюс Шнайер Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С, видання Триумф, 2002. – с. 170.

3. Баричев С.Г, Сєров Р.Е. Основы современной криптографии, видавництво Горячая линия - Телеком, 2002. – с.137-140.

4. О.М. Корков, М.В. Момот Оценка эффективности электронных денежных систем // Томський державний університет управління та радіоелектроніки, 2010. – с. 23.

5. О.Д. Вовчак Платіжні системи: навчальний посібник / О.Д. Вовчак, Г. Є. Шпаргало, Т.Я. Андрейків. - К.: Знання, 2008. – с. 38.

Надійшла: 15.12.2011

Рецензент: д.т.н., проф. Юдін О.К.