Старущенко М.В.
Національна академія Служби безпеки України

Безпека використання електронних грошей

За сучасних умов господарювання в практиці здійснення розрахунків між фізичними та юридичними особами все більшого поширення набуваються безготівкові платежі. Це пов'язано зі зручністю їх проведення, а також можливістю переказувати кошти не тільки в межах однієї країни, але й по всьому світу. У зв'язку з цим з'явились і продовжують виникати різноманітні платіжні інструменти, функціонування яких ґрунтується на використанні інноваційних технічних рішень, які отримали назву «електронні гроші» [1].

Сьогодні законодавче поле України щодо регулювання відносин пов'язаних із використанням електронних грошей складається із Закону України «Про платіжні системи та переказ коштів в Україні» від 05.04.2001 року, Закону України «Про електронну комерцію» від 03.09.2015 року, Постанови Правління НБУ «Про внесення змін до деяких нормативно-правових актів Національного банку України з питань 232 регулювання випуску та обігу електронних грошей» №481 від 04.11.2010 року, що затверджує Положення про електронні гроші [2].

Популярність використання електронних грошей в Україні з року в рік тільки зростає. Про це свідчать дані Національного банку України (табл.1). Так обсяг операцій електронних грошей за 1 півріччя 2016 року зріс майже у 1,6 рази порівняно з цим же періодом 2015 року, а кількість електронних гаманців зросла майже у 1,2 рази [3].

Таблиця 1. Порівняльний аналіз використання електронних грошей

Критерії порівняння	І півр. 2015	І півр. 2016
Обсяг операцій	1,1 млрд. грн.	1,8 млрд. грн.
Кількість електронних гаманців	36 млн.	43,6 млн.

Розробники вкладають великі кошти в забезпечення безпеки використання електронних гаманців. Однак вирішальну роль у збереженні свого електронного гаманця відіграє сам користувач. Постійне удосконалення механізмів захисту не може служити панацеєю, якщо власник електронного гаманця не дотримується елементарних правил безпеки.

Правила безпеки при використанні електронних гаманців

Використання віртуальної клавіатури. Щоб захистити електронні гроші, при введенні пароля на сайті електронної платіжної системи або в програмі електронного гаманця, необхідно використовувати віртуальну клавіатуру. Шахраї озброєні способами перехоплення сигналів з клавіатур, що дозволяють дізнатися діючий пароль, тому цю операцію краще довірити віртуальному аналогу звичайної клавіатури.

Перевірка протоколу сайта. Заходячи в особистий кабінет електронної платіжної системи, необхідно переконатися, що адресний рядок браузера показує необхідний сайт. Щоб не потрапити на шахрайський ресурс, потрібно перевірити наявність символів «https». Остання буква «S» повідомить користувачеві про наявність захисту, а значить він потрапить саме на сайт електронної платіжної системи.

Використання надійного пароля. Щоб доступ до електронного гаманця мав тільки його власник, пароль повинен бути максимально складним. Це ускладнить злом при використанні спеціальних програм, здатних перебирати багато варіантів паролів для входу в гаманець користувача.

Антивірусне програмне забезпечення. Щоб тримати в цілості електронні гроші, необхідно якомога частіше встановлювати нову версію антивірусного програмного забезпечення і проводити необхідні перевірки свого комп'ютера при виникненні такої потреби. Віруси найбільш часто зламують гаманці. Щоб подібне електронне шахрайство не позбавило користувача електронних грошей, антивірусне ПЗ повинне бути від надійного виробника.

Конфіденційність даних. Пароль від електронного гаманця, банківської карти, ніколи і ні за яких обставин нікому не повідомляють, навіть якщо хтось представляється співробітником банку або електронної платіжної системи. Реальні співробітники ніколи не будуть просити повідомити таку інформацію ні по телефону, ні по електронній пошті. Їх може вимагати тільки зловмисник.

Використання альтернативних носіїв пам'яті. Шкідливе програмне забезпечення (віруси) відкривають шахраям доступ до комп'ютерів користувачів і дозволяють завантажувати необхідні дані. Намагайтеся, не зберігати паролі в електронному вигляді на робочому комп'ютері. Використовуйте для цього флешку або інші альтернативні носії пам'яті і надійно ховайте їх від сторонніх людей.

Коди протекції. Коди протекції, ще один ефективний метод, що дозволяє захистити гроші. Практично всі електронні платіжні системи пропонують клієнтам подібний сервіс. Завжди використовуйте подібний захист електронного переказу, в цьому випадку нікому не вдасться перехопити його. Адже захисний код протекції знає тільки відправник і одержувач.

Прив'язка до IP адреса. Прив'язка віртуального гаманця до IP адресу значно підсилить безпеку аутентифікації користувача. Багато платіжних інтернет-систем надають таку можливість і цим треба користуватися, тому що увійти в обліковий запис елетронної платіжної системи можна буде тільки з цієї точки доступу в інтернет [4].

У зв'язку з стрімким розвитком електронних грошей в Україні – зростає і кількість кіберзлочинів у цій сфері. Користувачам, які використовують електронні гаманці для здійснення платежів потрібно бути обережними для збереження своїх електронних грошей. Дотримання вище зазначених правил дозволить суттєво підвищити рівень безпеки та не дозволить зловмиснику заволодіти вашим електронним гаманцем.

Список використаних джерел

1. *Носова Є. А. Використання інноваційних технологій для здійснення грошових розрахунків [Електронний ресурс] / Є. А. Носова. – 2015. – Режим доступу до ресурсу: http://ena.lp.edu.ua:8080/bitstream/ntb/32035/1/142-256-257.pdf;*
2. *Петрофанова К. Р. Правова природа електронних грошей [Електронний ресурс] / К. Р. Петрофанова // Національний юридичний університет імені Ярослава Мудрого. – 2016. – Режим доступу до ресурсу: http://dspace.nlu.edu.ua/handle/123456789/10075;*
3. *Електронні гроші [Електронний ресурс] // Національний банк України. – 2016. – Режим доступу до ресурсу: https://bank.gov.ua/doccatalog/document?id=26530351;*
4. *Как защитить электронные деньги [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://24paybank.com/faq/kak-zashitit-elektronnye-dengi.html.*