УДК 615.1:330.131

В.П. Клєпов,
викладач,
Херсонський політехнічний коледж Одеського національного політехнічного університету
vitalichpalich@gmail.com

Л.В. Єгоров,
студент,
Херсонський політехнічний коледж Одеського національного політехнічного університету

ДОСЛІДЖЕННЯ РИЗИКУ ВИКОРИСТАННЯ МОБІЛЬНИХ СИСТЕМ «БАНК-КЛІЄНТ»

В.П. Клєпов, Л.В. Єгоров. Дослідження ризику використання мобільних систем «банк-клієнт». Стаття дає аналіз найбільш поширених ситуацій виникнення ризикованих операцій з платіжними картками і заходи для мінімізації небезпеки для усіх основних учасників карткових розрахунків.

V.P. Klepov, L.V. Yegorov. The research of risk using mobile systems "Bank-client". The article gives the analysis of the most common situations of risk operations occurrence with payment cards and measures to minimize the risk for all stakeholders in the card payments.

Вступ. Сучасна банківська справа на Україні набирає все більше ознак цивілізованого ринку високо розвинутих країн Західної Європи та США. В операціях українських банків все частіше застосовуються новітні банківські технології.

Особливе місце в розвитку електронних банківських технологій посідає система “клієнт-банк”. Дана технологія є поширеною системою віддаленого доступу клієнтів до своїх банківських рахунків, але для приватних осіб банкомати ще довго будуть основним засобом дистанційного доступу до банку. Використання банкоматів Automatic Teller Machine (ATM) стало першою спробою банків надати клієнту можливість роботи із своїм рахунком у будь-який зручний для нього час і практично з будь-якого місця. Питання захисту інформації та інформаційної безпеки входять в зміст освіти молодшого спеціаліста, є актуальними на сучасному етапі розвитку людства. Таким чином, в змісті дисципліни «Безпека життєдіяльності» важливо приділяти увагу сукупності методів, засобів і заходів, спрямованих на уникнення ситуацій щодо спотворення, знищення і несанкціонованого використання накопичених, оброблених і збережених даних.

Постановка проблеми.

Будь-яка діяльність у середовищі банківського бізнесу набуває не тільки фінансового, інвестиційного, консультаційного характеру, а й

забезпечення конфіденційності інформації, а, отже, безпеки клієнтів. Використання розвинених електронних банківських технологій характеризується достатньо великим рівнем ризику, оскільки здійснення фінансових операцій часто пов'язане із невизначеністю, яка має як матеріальне, так і нематеріальне вираження.

З огляду на вище зазначене, **метою статті** є визначення кола ризиків з платіжними картками, виявлення розповсюджених проблем при роботі з банківськими картками й платіжними системами. Для її реалізації в процесі викладання дисципліни «Безпека життєдіяльності» нами визначено наступні **завдання:**

- провести моніторинг використання платіжних карток студентською молоддю;

- виявити ризики використання платіжних систем «банк-клієнт»;

- окреслити коло заходів щодо мінімізації ризиків для основних учасників роботи з картковими розрахунками.

Матеріал і результати дослідження. Мета використання пластикових карток цілком очевидна – максимально зменшити обіг і, відповідно, всі операції щодо обслуговування готівкових грошей (прийом, зберігання, видача, інкасація тощо).

Усі платіжні картки в Україні поділяються на кредитні та дебетні. Останні є безпосереднім представником активів клієнта банку, тому з них можна знімати та накопичувати кошти. Кожна операція з кредитною карткою (власне операція кредитування) збільшує борг клієнта перед банком чи торговою системою, який необхідно погасити з відповідними відсотками.

Також активно використовуються пластикові, магнітні та чіп-картки.

Пластикові картки випускаються (емітуються):

• окремими банками, великими торговельними фірмами – фірмові картки (локальні системи карток, Local);

• національними системами обігу карток (Domestic);

• міжнародними системами (International).

Другий тип карток - *магнітні картки.*

Вони позначаються стандартом ISO 7811. Інформація подається максимальним розміром у 1370 біт на 3-х смугах магнітної стрічки.

Основний недолік таких карток – досить велика ймовірність перемагнічування інформації та простий доступ до інформації з можливістю підробки. Для магнітних карток використовують переважно банкомати та платіжні автомати з on-line доступом.

Третій тип карток - *чіп-картки та смарт-картки*

Вони позначаються стандартом ISO 7816, мають автономний спеціалізований контролер доступу (чіп-картки) чи мікропроцесор (смарт-картки) та декілька видів електронної пам'яті. Обмін інформацією із банкоматом (пристроєм ініціалізації) здійснюється або через 8-контактну область, або є безконтактним. Картки можуть бути комбінованими, коли зворотна (безконтактна) сторона також містить магнітну смугу.

Для смарт-карток, як правило, вся система захисту будується засобами криптографії. Викрадені смарт-картки блокуються банкоматом відповідним записом у її пам'ять, сама ж картка після цього може повертатися "власнику".

Нові технології обману стали доступні насамперед завдяки широкому розповсюдженню банківських карт і онлайн-банкінгу.

За інформацією Національного банку України, в банківській системі України найбільш розповсюдженими є наступні види кіберзлочинів у сфері карткового бізнесу:

1) *Банкоматне шахрайство*:

- скімінг – виготовлення, збут та встановлення на банкомати пристроїв зчитування/копіювання інформації з магнітної смуги платіжної картки та отримання ПІН-коду до неї;
- використання «білого пластику» для «клонування» (підробки) платіжної картки та зняття готівки в банкоматах;
- Transaction Reversal Fraud – втручання в роботу банкомату при проведенні операцій з видачі готівки, яке залишає незмінним баланс карткового рахунку при фактичному отриманні готівки зловмисником;
- Cash Trapping – це заклеювання диспансеру банкомата для присвоєння зловмисником готівки, яка була списана з карткового рахунку законного утримувача картки.

2) *Шахрайські операції в торгівельно-сервісних мережах*:

- укладання фіктивних угод торговельного еквайрінгу для обслуговування підроблених платіжних карток; викрадення реквізитів платіжних карток, у тому числі також із застосуванням технічних засобів їх «клонування»;
- операції на суму нижче встановленого ліміту без проведення авторизації; використання у платіжних системах втрачених/викрадених/підроблених платіжних карток.

3) *Шахрайство в мережі Інтернет*:

- викрадення реквізитів платіжних карток;
- проведення операцій із використанням викрадених реквізитів платіжних карток;

- діяльність щодо створення програмних засобів для викрадення реквізитів платіжних карток (фітинг – створення фіктивних WEB-сайтів та здійснення фальсифікованої інформаційної розсилки повідомлень, поширення комп'ютерних вірусів та троянських програм, перехоплення трафіку тощо).

4) *Шахрайські схеми в системах дистанційного банківського обслуговування (далі – ДБО)*:

- впровадження комп'ютерних вірусів та троянських програм для прихованого перехоплення управління ПК клієнта з встановленим програмним забезпеченням ДБО (віруси типу Gamker і Carberp, банківські трояни для крадіжки інформації (Neverquest));
- відкриття рахунків, проведення несанкціонованих операцій та отримання готівки в результаті неправомірних операцій у системах ДБО;
- незаконне отримання платежів від закордонних відправників через міжнародну систему SWIFT внаслідок втручання у роботу комп'ютерів та клієнтських систем ДБО закордонних банків.

Як приклад розглянемо більш детально один з виділених нами типів кіберзлочинів у сфері карткового бізнесу.

Скімінг (від англ. skim - знімати вершки) - різновид шахрайства з платіжними картками, при якому на банкомат встановлюється спеціальний пристрій (скімер). Скімінговий пристрій - це електронний пристрій, який прикріплюється до отвору для введення картки в банкомат для зчитування персональної інформації з магнітної стрічки банківської картки клієнта (Рис. 1). Щоб дізнатися PIN-код, шахраї встановлюють на банкомати міні-камери і накладки на клавіатуру (Рис. 2). Після цього злочинці мають доступ до карткових рахунків громадян.

Рис. 1. Накладні клавіатури, та спеціальний пристрій (скімер).

Рис. 2. Прихована камера у скриньці для реклами.

За інформацією прес-служби МВС, очевидною є тенденція щодо зростання використання шахрайських пристроїв. Так, у 2013 році було

виявлено близько 160 скімінгових пристроїв на банкоматах, в 2012 р. – 73, у 2011 р. – 45.

Для проведення аналізу досвідченості студентів щодо правил користування платіжними картками та можливості виникнення ризикових операцій за допомогою платіжних систем, було опитано студентів Херсонського політехнічного коледжу Одеського національного політехнічного університету.

Випадки фізичної крадіжки банківської карти мали місце лише у 5% опитаних. Результати відповідей на питання «Чи буде вважатися надійним тривале збереження ваших кошт на банківській картці?» 56% відповіли «так» (Рис. 3).

Щодо питання «Чи знаєте Ви правила безпечного використання банківських карт?» - 89,2% відповіли - «ні» (Рис. 4). Це свідчить про те, що працівники банку не ознайомлюють користувачів карток з можливими ризиками використання мобільних систем «банк-клієнт», також мало приділяється уваги цьому питанню дорослими (батьками студентів, викладачами, класними керівниками) для роз'яснення ситуацій та правил користування карток.

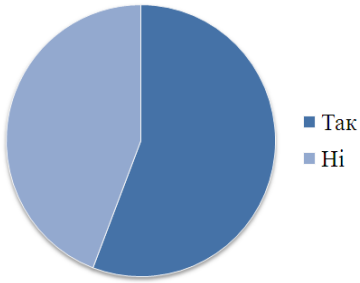

Рис.3. Результати відповідей на питання «Чи буде вважатися надійним тривале збереження ваших кошт на банківській картці?»

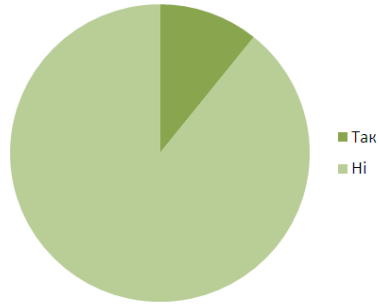

Рис.4. Результати відповідей на питання «Чи знаєте Ви правила безпечного використання банківських карт?»

Відповіді на питання «Якщо у Вас з карти було знято готівку, як Ви про це дізналися?» дають чітку уяву про те, що користувачі карток не володіють інформацією про залишок коштів на картці, але 60% опитаних контролюють баланс за допомогою послуги СМС-повідомлення.

На запитання «Чи мали Ви у своїй практиці ситуацію пов'язану з некоректною роботою банкомату чи терміналу?» - 20% респондентів відповіли «так». Це свідчить про те, що система роботи банкоматів є

недосконалою, адже будь-які електронні системи потребують удосконалення і якісної, професійної технічної підтримки.

Аналіз результатів анкетування дозволив сформулювати наступні рекомендації, які допоможуть користувачу зберегти персональні дані банківської картки та кошти на її рахунку:

1. Отримання готівкових грошей за допомогою банкомату повинно проводитися в режимі самообслуговування.

2. Перед роботою з банкоматом необхідно звернути увагу на наступне:

- при появі на банкоматі додаткових пристрої, що не відповідають його зовнішньому вигляду, знімати кошти там не варто;
- при наборі коду прикривайте клавіатуру вільною рукою, сумкою чи гаманцем;
- намагайтеся не знімати кошти з картки вночі, бо зазвичай встановлення скімінгових пристроїв відбувається у вечірній час, коли служби безпеки банків не здійснює моніторинг пристроїв.

3. Для цілодобового контролю варто підключити послугу СМС-інформування.

4. Ні слід повідомляти паролі карток тому, хто бажає перевести вам гроші. Для зарахування коштів на рахунок згода не потрібна.

5. Через конфіденційність інформації про власника картки, рекомендується забирати з собою роздрукований чек і ніколи не залишати його біля банкомату.

6. Те ж саме стосується і сайтів, які можуть нагадувати сторінку вашого банку. Часто шахраї роблять схожі сторінки, щоб виманювати персональні дані клієнтів банків.

7. Намагайтеся не випускати картку з виду, коли розраховуєтесь. Навіть у ресторанах вже використовуються мобільні термінали, які офіціанти повинні приносити до вашого столу.

8. Систематично перевіряйте свій комп'ютер на наявність вірусів, бо деякі з них збирають інформацію про дані платіжних карт і надсилають їх шахраям.

9. У випадку вилучення банкоматом Вашої картки, необхідно терміново зателефонувати до Банку та заблокувати свою картку.

Висновок. Останнім часом за допомогою пластикової картки можна сплатити за покупки в магазині, комунальні послуги, поповнити баланс на мобільному телефоні, банк може видати безготівковий кредит. Асортимент послуг збільшується, при цьому зростають ризики використання платіжних систем. Акцентування уваги на проблемах та можливих ризиках при користуванні платіжними картками серед молоді

повинно сприяти формуванню їх інформаційної, фінансової грамотності та банківської культури суспільства.

Розуміння ризиків, що виникають при здійсненні електронних розрахунків, зокрема шахрайства з платіжними картками, та реалізація ефективної політики управління такими ризиками, дає змогу не тільки забезпечити фінансову стійкість і стабільну роботу банків, а й підвищити довіру населення до банківського сектора України загалом та всіх форм карткових розрахунків зокрема.

Результати даного дослідження можуть бути використані викладачами та студентами не тільки при вивченні дисципліни «Безпека життєдіяльності», а й у повсякденному житті з метою безпечного користування платіжними системами.

Література

1. Банківський сектор активно інвестує у розвиток карткового бізнесу [Електронний ресурс]. – Режим доступу: http:// www.siogodennya.org.ua/?p=19602 – назва з екрану.

2. В Україні зростає фінансова кіберзлочинність [Електронний ресурс].– Режим доступу: http://news.finance.ua/ ua/~/2/0/all/2013/12/15/314801 – назва з екрану.

3. Вядрова Н.Г. Шляхи протидії шахрайствам у сфері електронних розрахунків [Електронний ресурс] – Режим доступу: http://univd.edu.ua/general/publishing/konf/ finbezpeka/24_vyadrova.pdf.

4. Колдовський М.В. Ризики використання банківських платіжних карток / М.В. Колдовський, О.М. Ващенко // Вісник Української академії банківської справи. – 2010. – № 1. – С. 45–49.

5. Круглый стол «Киберпреступность: украинские банки на линии удара» (информационно-аналитические материалы) [Електронний ресурс]. – Режим доступу: http://lfr.org.ua/ru/analytics/822-2013-26-11-analytics.html – назва з екрану.

6. Мельник Ю.Б. Ризики у сфері банківського карткового бізнесу / Ю.Б. Мельник. – [Електронний ресурс]. – Режим доступу: http:// www.cibs.ck.ua/parts/scien/stconf/10/tezy.pdf.

7. Моніторинг шахрайських операцій [Електронний ресурс]. – Режим доступу: http://www.ufn.com.ua/monitoring_ fraud.html?lang=ua – назва з екрану.

Надійшла до редакції 11.12.2015