DOI: https://doi.org/10.32782/2524-0072/2018-18-116

УДК 303.09:336.717.1

Аналіз наслідків кібершахрайств в банківській системі України[1]

Яровенко Г.М.
кандидат економічних наук,
доцент кафедри економічної кібернетики
Навчально-наукового інституту бізнес-технологій «УАБС»
Сумського державного університету

Бояджян М.М.
студент
Навчально-наукового інституту бізнес-технологій «УАБС»
Сумського державного університету

Стаття присвячена актуальним питанням боротьби із кібершахрайствами в банківській сфері. Проаналізовано наслідки шахрайств щодо операцій з банківськими картками для банків та їх клієнтів. Це дозволило виділити найбільш активні способи шахрайства такі, як соціальну інженерію та Інтернет-шахрайства. Для боротьби з даним явищем запропоновано: створення алгоритмів відслідковування шахрайських операцій із використанням Data Mining, розробку автоматизованого модулю моніторингу, вбудованого в банківську систему та різні платіжні системи, розробку інтегрованого банку даних, організаційні та соціальні заходи.

Ключові слова: кібершахрайство, банк, клієнт, платіжна картка, соціальна інженерія, фішинг, вішинг, Data Mining, інформаційні технології.

Яровенко А.Н., Бояджян М.М. АНАЛИЗ ПОСЛЕДСТВИЙ КИБЕРМОШЕННИЧЕСТВ В БАНКОВСКОЙ СИСТЕМЕ УКРАИНЫ

Статья посвящена актуальным вопросам борьбы с кибермошенничествами в банковской сфере. Проведен анализ последствий мошенничеств по операциям с банковскими карточками для банков и их клиентов. Это позволило выделить наиболее активные способы мошенничества, такие как социальную инженерию и Интернет-мошенничества. Для борьбы с данным явлением предложено: создание алгоритмов отслеживания мошеннических операций с использованием Data Mining, разработку автоматизированного модуля мониторинга, встроенного в банковскую систему и различные платежные системы, разработку интегрированного банка данных, организационные и социальные мероприятия.

Ключевые слова: кибермошенничество, банк, клиент, платежная карточка, социальная инженерия, фишинг, вишинг, Data Mining, информационные технологии.

Yarovenko H.M., Boiadzhian M.M. ANALYSIS OF THE CYBER FRAUD CONSEQUENCES IN THE BANKING SYSTEM OF UKRAINE

The article is devoted to topical issues of the fight against cyber fraud in the banking sector. It was analyzed the fraud impact on the operations with bank cards for banks and their customers. It allowed us to identify the most active methods of fraud, such as social engineering and Internet-fraud. To fight this phenomenon, it was proposed: the creating algorithms for tracking fraud operations with using Data Mining, the development of an automated monitoring module which is embedded in the banking system and different payment systems, the development of an integrated data bank, the organizational and social activities.

Keywords: cyberfraud, bank, client, payment card, social engineering, phishing, vishing, data mining, information technologies.

Постановка проблеми у загальному вигляді. Сьогодні питання боротьби з кібершахрайством є актуальним в Україні, оскільки дана проблема торкається різних суб'єктів – держави, банків, суб'єктів господарювання та населення. Не дивлячись на проведення різних активних заходів, робота в цьому напрямку не є системною. Кожний банк впроваджує свої заходи та програмне забезпечення, які за часту не є ефективними; НБУ здійснює тільки регламентацію положень та формує рекомендації щодо створення системи захисту. В резуль-

[1] Робота виконана в рамках держбюджетної науково-дослідної роботи № 0118U003574 «Кібербезпека в боротьбі з банківськими шахрайствами: захист споживачів фінансових послуг та зростання фінансово-економічної безпеки України»

тати населення стає все частіше об'єктом шахрайств, втрачає довіру до банків, як фінансових інститутів, що призводить до втрати банками клієнтів.

В Україні за 2017 рік кібершахраями було вкрадено 670 млн грн., а у 2016 році майже удвічі менше – 339 млн грн. Це свідчить про те, що заходи кібербезпеки, організовані у банках, не є досить ефективними. Хоча дану проблему широко популяризують через засоби масової інформації, проводиться роз'яснювальна робота з даного питання серед населення, але випадки шахрайств все одно зростають. Методи шахраїв модифікуються, що потребує також модифікації системи захисту в банках.

Тому вирішення даної проблеми потребує інтеграції зусиль всіх учасників та формування більш ефективних та сучасних підходів до організації системи безпеки. Для цього необхідно здійснювати моніторинг операцій, аналізувати способи та інструменти шахрайства, досліджувати ситуації, в яких було здійснено шахрайство. В результаті можна отримати інформацію стосовно того, як діє шахрай та його жертва, та визначити способи, які можна використати для попередження даного роду кібершахрайств.

Ця проблема досить актуальна для банків та їх клієнтів, особливо в частині здійснення ними операцій за допомогою банківських карток, які за останні роки набули масового розповсюдження для проведення платіжних, кредитних, депозитних та інших операцій. Тому в даній статті буде проведено аналіз наслідків для банків та їх клієнтів в результаті застосування різного роду шахрайств щодо операцій з банківськими картками.

Аналіз останніх досліджень і публікацій. Проблематикою кібершахрайств у банківській сфері займаються останні 10-15 років, що пов'язано із зростанням науково-технічного прогресу в галузі інформаційних технологій та програмного забезпечення, а також із збільшенням доступності до інформації з боку звичайного користувача. Так, типологія суб'єктів фінансового шахрайства в комерційних банках досліджувалася в наукових працях Д.Н. Козлова, В.В. Левіна, Н.С. Подосенка, О. Саяпіна, А.М. Шевченка та інших. Способи новітніх шахрайських операцій в банківський сфері представлені в працях О.В. Кришевича, С.В. Поперешняка, С.В. Шапочки та інших. Що стосується способів боротьби із шахрайствами у банках, то питаннями застосування сучасних методів математичного моделювання та автоматизованих інформаційних систем для вирішення питань кібербезпеки, займалися вітчизняні та закордонні фахівці: J. Dean, S. Guido, W. Meira, A.S. Muller, J. Stanton, M.J. Zaki, Е. Балдін, П. Волкова, А. Коробєйніков, С. Мастицький, Н. Паклін, В. Орешков, В. Шитіков, А. Шипунов та інші.

Незважаючи на велику кількість праць у даній сфері, не проаналізовано наслідки для банківської системи в результаті кібершахрайств та відсутні конкретні рекомендації щодо удосконалення банківської системи кіберзахисту.

Виділення невирішених раніше частин загальної проблеми. Банківська система є однією з головних ланок фінансово-кредитної системи країни. За часту вона є одним з об'єктів, які приваблюють шахраїв та злочинців, що підриває авторитет банків, як гарантів збереження та накопичення коштів населення, держави та суб'єктів господарювання. Способи шахрайств модифіковуються, відповідно банківські служби кібербезпеки не встигають удосконалювати методи боротьби з ними. Тому аналіз наслідків з урахуванням впливу різних способів шахрайств для банківської системи дасть можливість розробити план майбутніх інструментів та способів попередження кібершахрайств.

Формулювання цілей статті. Метою даної статті є аналіз наслідків в результаті здійснення різного роду кібершахрайств в банківській системі в частині проведення операцій з платіжними картками, та формування можливих напрямів для організації їх виявлення та попередження за допомогою математичних інструментів та інформаційних технологій.

Виклад основного матеріалу дослідження. Впровадження банківських карт і використання комп'ютерних технологій в сфері платежів є характерною рисою повсякденного життя. Швидкими темпами розвиваються безготівкові форми розрахунків. Платежі, що здійснюються без участі готівки, сприяють прискоренню оборотності, скороченню кількості грошових коштів, необхідних в обігу, що, як наслідок, призводить до зниження витрат обігу, збільшенню прозорості розрахунків [1]. Завдяки своєї простоти, масовості, доступності технологій, операції з банківськими картками найбільш приваблюють шахраїв.

З 01.01.2017 по 26.08.2017 платіжні сервіси системи Exchange-Online зафіксували 12416 підозрілих операцій на загальну суму 3409000 гривень. В операціях прийняло участь 7390 банківських карт 135 банків з 53 країн, в тому числі з 67 українських банків. Дані кошти

шахраї намагалися вивести за допомогою мобільних пристроїв [2].

На рисунку 1 представлено країни, за картками яких проводились спроби операцій, ідентифікованих системою, як шахрайська, та відсоток операцій, які дійсно виявилися шахрайськими.

Дані рисунку 1 свідчать про те, що Україна займає лідуюче місце та втрапила в п'ятірку країн, в яких банківські платіжні операції є не досить захищеними. Виявилося, що 19% операцій є дійсно шахрайськими і це перевищує обсяги шахрайств в інших країнах. За допомогою кібершахрайств з карток українців було знято 238955 гривень. Тобто, банківські платіжні системи через слабкий захист потенційно можуть втрачати клієнтів через той факт, що вони можуть стати об'єктами шахрайства. Тому це не тільки проблема банків, але й соціальна проблема, яку треба вирішувати комплексно та із залученням різних структур – держави, населення, банків, інвесторів.

На сьогоднішній день найбільш поширеними видами шахрайських операцій з банківським картками є:

– скімінг – викрадення інформації з магнітної стрічки картки або ПІН-коду за допомогою спеціальних пристроїв;

– трапінг – встановлення пасток на шатер банкомату;

– фізичне пошкодження банкоматів;

– фішинг – шахрайство за допомогою Інтернету;

– вішинг – шахрайство за допомогою мобільного зв'язку;

– вірусні та хакерські атаки, тощо.

На рисунку 2 наведені групи шахрайських операцій, здійснених за 1 півріччя 2017 року та об'єднаних за однаковим способом здійснення, які представлені у відсотках.

Найбільша доля шахрайських операцій, які було здійснено за допомогою методів соціальної інженерії (41%), включають в себе здійснення вішингу та фішингу, тобто шахраї виманюють дані платіжних карток у клієнтів, отримують доступ до рахунків та знімають кошти. Зазвичай жертвами соціальної інженерії стають літні люди (від 55 і старші) – 15%, і середнього віку (35-44) – 13%.

Досить популярними у шахраїв є способи крадіжок коштів через банкомат (32%) та через Інтернет (16%) (див. рис. 2). Тобто, банківська система кібербезпеки повинна розробити додаткові способи захисту операцій від цих видів шахрайств.

Шахрайство шляхом соціальної інженерії – це глобальна проблема. Станом на кінець пер-

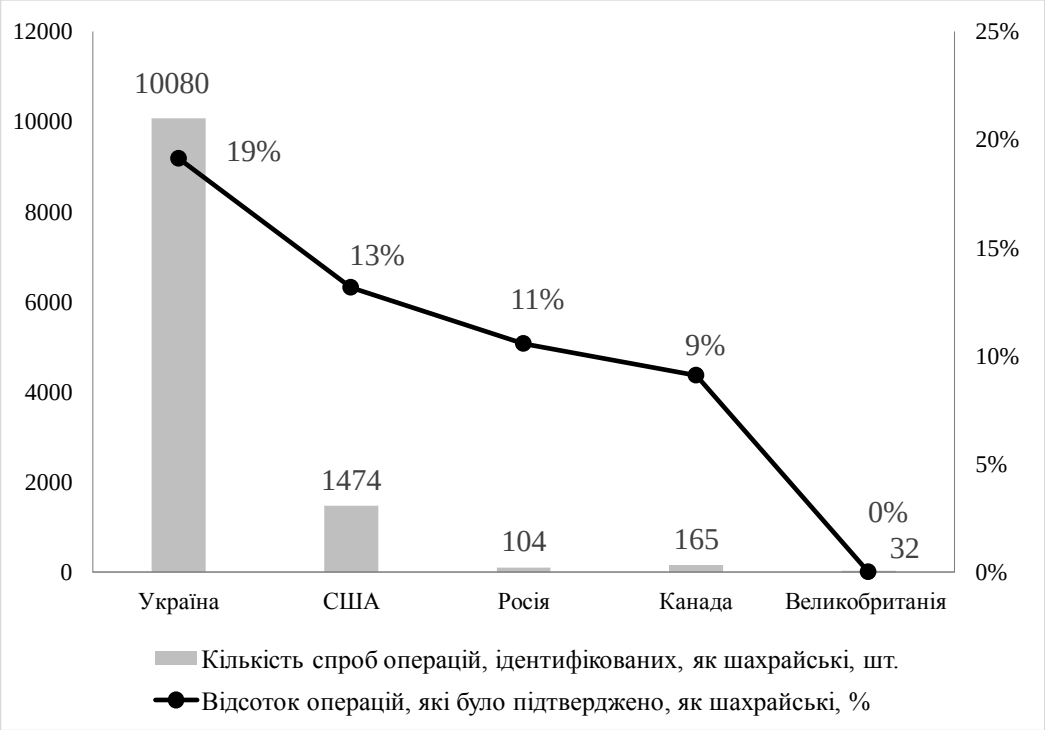

Рис. 1. Аналіз шахрайських операцій, здійснених у 2017 році

Джерело: побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем [2]

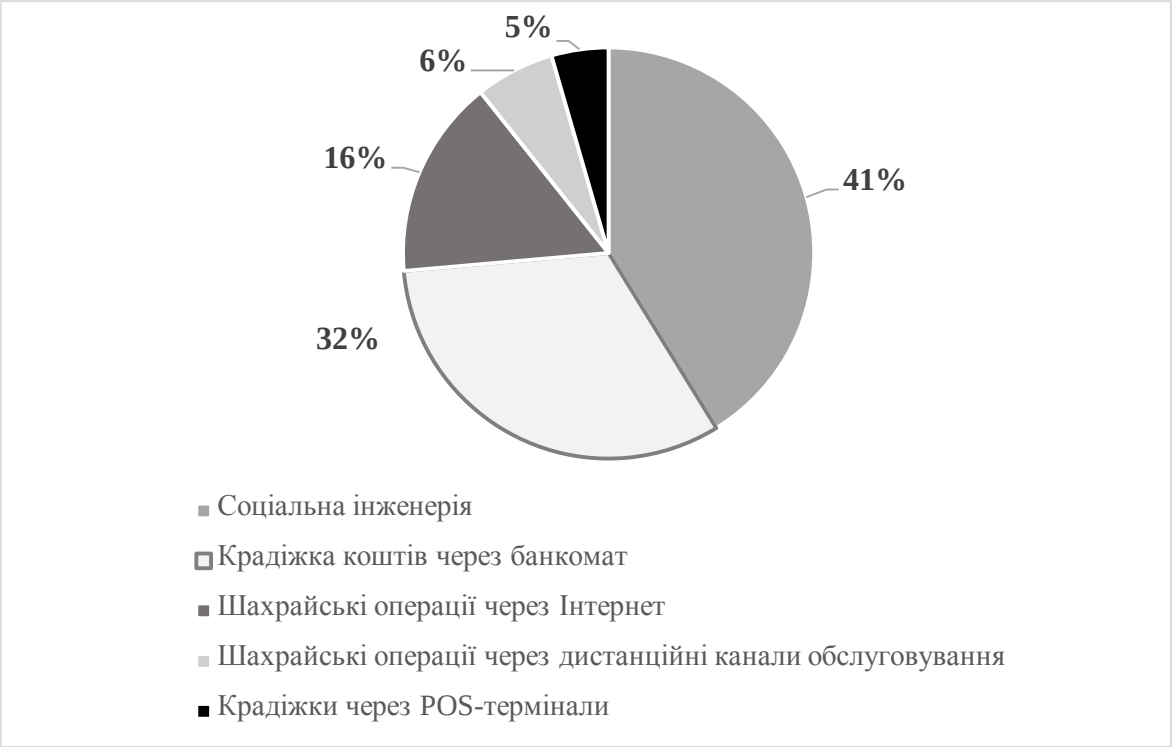

Рис. 2. Групи шахрайських операцій, об'єднаних за однаковим способом здійснення

Джерело: побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем [3]

шого кварталу 2017 року найбільшої шкоди від фішингових атак зазнали 51,70% банків світу. До країн з найвищим відсотком нападу на користувачів відносяться: Китай (20,87%), Бразилія (19,16%), Макао (11,94%), Російська Федерація (11,29%), Австралія (10,73%), Аргентина (10,42%), Нова Зеландія (10,18%), Катар (9,87%), Казахстан (9,61%), Тайвань (9,27%). За часткою атакованих користувачів від вішингу до найбільш атакованих країн відносяться: Росія (1,2%), Узбекистан (0,40%), Казахстан (0,36%), Таджикистан (0,35%), Туреччина (0,34%), Молдова (0,31%), Україна (0,29%), Киргизстан (0,27%), Білорусь (0,26%) та Латвія (0,23%) [4].

В Україні у 2017 року збитки клієнтів банків від соціальної інженерії склали 509,72 млн грн., що практично вдвічі перевищило збитки за 2016 рік та у 9 разів за 2015 рік. Також збільшилася середня сума шахрайської операції, здійсненої за допомогою методів соціальної інженерії, до 2543 грн. у 2017 році, що в 1,8 разів перевищує даний показник у 2016 році (див. табл. 1).

В Україні найбільша кількість випадків платіжного шахрайства з використанням методів соціальної інженерії здійснюється в середовищі Card-Not-Present (операції здійснюються без наявності картки та фізичної присутності користувача), у порівнянні із обслуговуванням через банкомати, POS-термінали та дистанційне банківське обслуговування (див. рис. 3).

Методи соціальної інженерії набирають популярності у шахраїв, оскільки зловмисники не тільки отримують дані платіжної картки, але й ідентифікаційні дані клієнта. Також даний спосіб шахрайства є досить простим у здійсненні. Хоча банківські співробітники й попереджають своїх клієнтів не розголошувати платіжну інформацію через телефон, але шахраї мають досить багато способів психологічного впливу на жертву.

На основі проведеного аналізу наслідків кібершахрайств, які відбуваються в сфері використання клієнтами банків платіжних засобів, найбільш вразливим місцем є сам клієнт, який під дією різних методів соціальної інженерії становиться об'єктом шахрайства. Для боротьби з даним способом шахрайства українські банки не мають досить дієвих інструментів. На нашу думку, для даного випадку шахрайства доцільно застосовувати сукупність засобів, що базуються на методах інтелектуального аналізу та інформаційних технологій.

Автори статті вбачають організацію наступних заходів для боротьби із кібершахрайствами, особливо соціальною інженерією:

1) доцільно побудувати алгоритми із використанням інструментів Data Mining, за допомогою яких відбуватиметься відслідковування операцій та перевірка їх на предмет шахрайства у відповідності з певними ознаками. Дана проблематика розкрита авторами даної статті у роботі [8]. Особливо дієвим є застосування нейронних мереж, що дозволить постійно налаштовувати систему на нові ознаки шахрайства. Тобто у випадку, коли шахрай знімає всю суму коштів з рахунку, то система здійснює перевірку даної операції. У випадку шахрайства операція блокується;

2) розробка автоматизованого модулю моніторингу, вбудованого в банківську систему та різні платіжні системи, функція якого – автоматична перевірка операцій на предмет шахрайства, блокування операцій та подвійна (потрійна) ідентифікація клієнта. Частково це реалізовано в існуючих платіжних системах, але у випадках соціальної інженерії системи не працюють. Коли система блокує операцію з ознаками шахрайства, то вона повинна надіслати клієнту повідомлення, в якому вказується тип операції з вказівкою місця її здійснення та суми. Наприклад, якщо шахрай

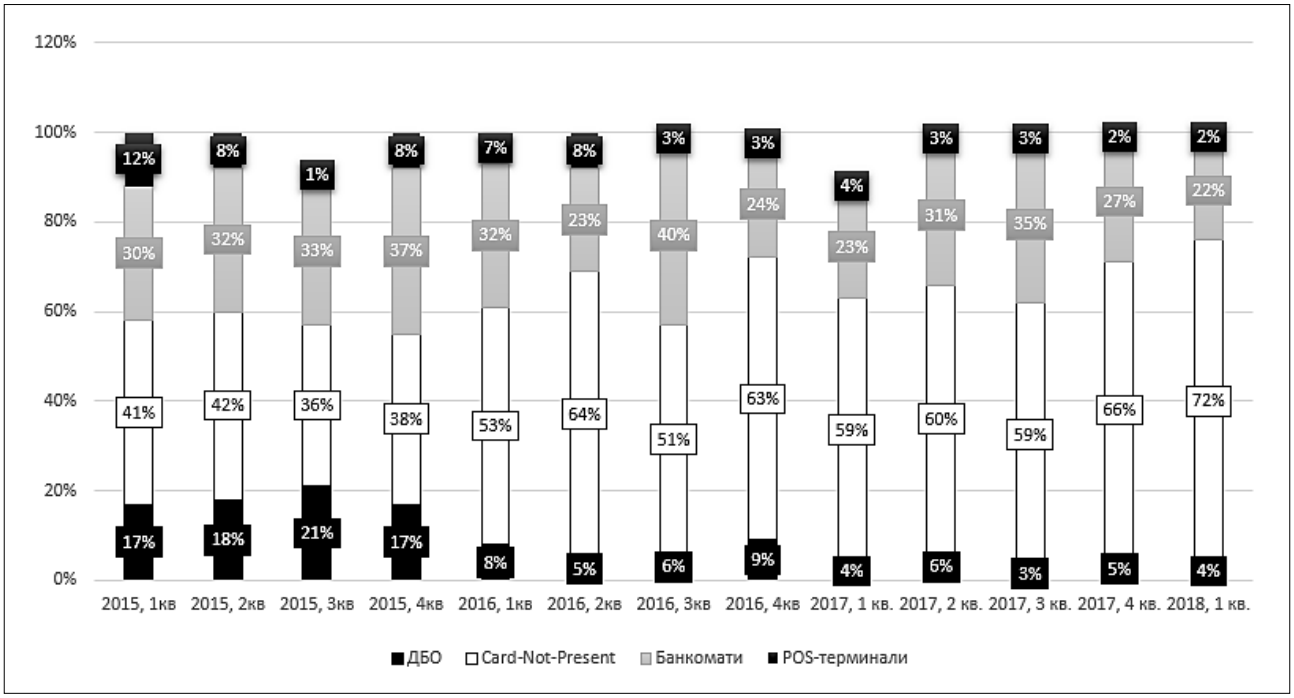

Рис. 3. Шахрайські операції за різними видами банківського обслуговування

Джерело: побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем [7]

Таблиця 1

Збитки від шахрайських операцій, здійснених за допомогою соціальної інженерії та засобів Інтернет

Вид збитку	2015		2016		2017	
	Соціальна інженерія	Інтернет	Соціальна інженерія	Інтернет	Соціальна інженерія	Інтернет
Середня сума збитку від однієї шахрайської операції, грн.	834	206	1403	345	2543	145
Загальні збитки від шахрайських операцій, млн. грн.	51,74	32,62	275,45	63,68	509,72	159,91

Джерело: побудовано на основі даних Української міжбанківської Асоціації членів платіжних систем [5; 6]

знаходиться в іншій країні, то клієнту надходить повідомлення, що є спроба зняття з його рахунку коштів на вказану суму із вказаної країни. Якщо клієнт не ініціював операцію, то він повинен надіслати банку код з відміною або з блокуванням;

3) створення інтегрованого банку даних, який буде містити інформацію щодо: способу, методу, виду шахрайства, характерних ознак, характеристик шахрая та його жертви, мобільні телефони, IP-адреси шахраїв, тощо. Дана інформація дозволить формувати нові правила перевірки та контролю банківських операцій на предмет відповідності ознакам шахрайства. Подібні бази повинні створюватися не для окремих банків, а для всієї банківської системи, оскільки дана інформація є типовою;

4) жорстке обмеження прав доступу працівників банків до бази даних клієнтів для зменшення шахрайств з боку працівників. Це можливе за рахунок чіткого розмежування прав доступу до інформації, налаштованого на програмному рівні. Даний підхід потребує створення та модифікацію посадових інструкцій працівників банків та розробку інструкцій та рекомендацій головних банків та Національного банку України;

5) збільшити кількість інструментів соціальної роботи із населенням через засоби масової інформації та Інтернет для зменшення випадків соціального шахрайства. Це сприятиме формуванню ефективної системи взаємодії між банками та клієнтами.

Висновки з проведеного дослідження. Таким чином, здійснення кібершахрайських операцій з банківськими картками та різними платіжними операціями має негативні наслідки для стабільності фінансової системи держави. Це проявляється у гальмуванні поширення безготівкової форми оплати, зниженні довіри населення до банків у частині зберігання коштів та кредитування. Недостатні знання про механізми кіберзлочинів ускладнюють процес визначення шахрайства. Вивчення ознак шахрайства, в першу чергу, необхідно для розробки більш дієвих засобів і методів захисту від даного виду злочину. Аналіз наслідків кібершахрайств дозволяє виявити слабкі місця в банківській системі та сприяє накопиченню інформації щодо способів, методів шахрайства, портретів шахраїв та їх жертв, формування ознак шахрайства.

В результаті проведеного в статті аналізу виявлено, що збитки банків в результаті кібершахрайств зростають, не дивлячись на заходи служб безпеки. Клієнти та банки втрачають кошти завдяки різним шахрайським способам, серед яких найбільшої шкоди завдають методи соціальної інженерії. Для боротьби з такого роду шахрайствами запропоновано ряд заходів, реалізація яких потребує застосування методів Data Mining та розвинутих інформаційних технологій.

ЛІТЕРАТУРА:

1. Кривошапова С. В., Литвин Е. А. Оценка и способы борьбы с мошенничеством с банковскими картами. Международный журнал прикладных и фундаментальных исследований. 2015. № 4. С. 116–120.

2. Fraud Digest 28.09.2017 [Електронний ресурс] // Украинская межбанковская ассоциация членов платежных систем EMA. – 2017. URL: https://ema.com.ua/fraud-digest-28-09-2017.

3. Fraud Digest 28.07.2017 [Електронний ресурс] // Украинская межбанковская ассоциация членов платежных систем EMA. – 2017. URL: https://ema.com.ua/fraud-digest-25-07-2017/.

4. Trend Report “Financial Cyber Threats Q1 2017» [Електронний ресурс] // The official site of the company “ElevenPaths”. 2017. URL: https://www.elevenpaths.com/wpcontent/uploads/2017/04/Financial_Threats_Q1-2017_EN.pdf.

5. Статистика платежного мошенничества – итоги 2017-го года [Електронний ресурс] // Украинская межбанковская ассоциация членов платежных систем EMA. 2017. URL: https://ema.com.ua/cyberfraud-ema-statistics-results-2017.

6. Некрасов В. Українці збагатили кібершахраїв на півмільярда: як не стати жертвою [Електронний ресурс]. FINANCE.UA. 2018. URL: https://news.finance.ua/ua/news/-/419603/ukrayintsi-zbagatyly-kibershahrayiv-na-pivmilyarda-yak-ne-staty-zhertvoyu.

7. Підсумки квартального засідання Форуму безпеки розрахунків з платіжними інструментами та кредитами 25 травня 2018р. [Електронний ресурс] // Украинская межбанковская ассоциация членов платежных систем EMA. 2018. URL: https://ema.com.ua/summary-fbrik-may-2018.

8. Яровенко Г. М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу [Електронний ресурс] / Г. М. Яровенко, А. І. Сковронська, М. М. Бояджян // Ефективна економіка. 2018. № 7. URL: http://www.economy.nayka.com.ua/?op=1&z=6453.

REFERENCES:

1. Krivoshapova S. V., Litvin, E. A. (2015) Otsenka i sposoby bor'by s moshennichestvom s bankovskimi kartami [Evaluation and ways to combat bank card fraud]. International Journal of Applied and Basic Research, vol. 4, pp. 116-120.

2. The official site of the Ukrainian Interbank Association of Members of EMA payment systems (2017), “Fraud Digest 28.09.2017”, available at: https://ema.com.ua/fraud-digest-28-09-2017 (accessed 18 October 2018).

3. The official site of the Ukrainian Interbank Association of Members of EMA payment systems (2017), “Fraud Digest 28.07.2017”, available at: https://ema.com.ua/fraud-digest-25-07-2017/ (accessed 18 October 2018).

4. The official site of the company “ElevenPaths” (2017), “Trend Report “Financial Cyber Threats Q1 2017””, available at: https://www.elevenpaths.com/wp-content/uploads/2017/04/Financial_Threats_Q1-2017_EN.pdf (accessed 18 October 2018).

5. The official site of the Ukrainian Interbank Association of Members of EMA payment systems (2017), “Payment fraud statistics – results of 2017”, available at: https://ema.com.ua/cyberfraud-ema-statistics-results-2017 (accessed 18 October 2018).

6. Nekrasov V. (2018) Ukrajinci zbaghatyly kibershakhrajiv na pivmiljjarda: jak ne staty zhertvoju [Ukrainians have enriched cyber shields for half a billion: how not to become a victim]. FINANCE.UA (electronic journal), vol. 7, available at: https://news.finance.ua/ua/news/-/419603/ukrayintsi-zbagatyly-kibershahrayiv-na-pivmilyarda-yak-ne-staty-zhertvoyu (accessed 18 October 2018).

7. The official site of the Ukrainian Interbank Association of Members of EMA payment systems (2018), “Results of the quarterly meeting of the Forum for settlement of securities with payment instruments and loans May 25, 2018”, available at: https://ema.com.ua/summary-fbrik-may-2018 (accessed 18 October 2018).

8. Yarovenko H.M., Skovronska A.I., Boiadzhian M.M. (2018) Modeljuvannja vyjavlennja oznak kiberzaghroz v bankakh iz vykorystannjam intelektualjnogho analizu [Modeling the detect signs of the cyber threats in the banks with using data mining]. Efektyvna ekonomika [Effective economy] (electronic journal), vol. 7, available at: http://www.economy.nayka.com.ua/?op=1&z=6453 (accessed 18 October 2018).

Analysis of the cyber fraud consequences in the banking system of Ukraine

Yarovenko H.M.
Candidate of Economic Sciences, Associate Professor,
Educational and Scientific Institute of Business Technologies
"UAB" of Sumy State University

Boiadzhian M.M.
Student
Educational and Scientific Institute of Business Technologies
"UAB" of Sumy State University

The issue of the fight against cyber fraud is very relevant in Ukraine. Ukrainian banks implement different measures and software that are not effective. As a result, the population is increasingly subject to fraud and loses their confidence in banks, which leads to financial losses. The purpose of the article is the analysis of the consequences as a result of the different types implementation of cyber fraud in the banking system, especially in the area of operations with payment cards, and the formation of possible directions for the organization of their detection and prevention. Ukraine ranks the first place among five countries where bank payment transactions are not sufficiently protected. It turned out that 19% of transactions are really fraudulent and it exceeds the amount of fraud in other countries. The largest fraction of fraudulent operations in Ukraine (41%) is related to operations carried out using social engineering methods. The methods of fraud through ATM (32%) and the Internet (16%) are also quite popular with fraudsters. The losses of Ukrainian banking clients from social engineering amounted to 509.72 million UAH in 2017, which exceeded the losses almost by half in 2016 and by 9 times in 2015. In Ukraine, the largest number of payment fraud cases with using the methods of social engineering is carried out in the medium of Card-Not-Present. The results of the analysis show that exactly the bank client is the most vulnerable part, which becomes the object of fraud under the influence of various methods of social engineering. Ukrainian banks do not have sufficiently effective tools to fight against this type of fraud. To resist this phenomenon, authors proposed: the creating algorithms for tracking fraud operations with using Data Mining, the development of an automated monitoring module which is embedded in the banking system and different payment systems, the development of an integrated data bank, the organizational and social activities.