УДК 336.717

Домінова І.В.,
аспірант кафедри менеджменту банківської діяльності,
Київський національний економічний університет імені Вадима Гетьмана

РИЗИК ШАХРАЙСТВА В УМОВАХ ФУНКЦІОНУВАННЯ ЕЛЕКТРОННОГО БАНКІНГУ

Домінова І.В. Ризик шахрайства в умовах функціонування електронного банкінгу. У статті розглянуто сутність та об'єкти ризику шахрайства в умовах функціонування електронного банкінгу. Виявлено основні джерела ризику шахрайства під час електронного банківського обслуговування. Описані найбільш поширені види шахрайства з платіжними картками. Розглянуто види шахрайства з мобільним телефоном, Інтернетом та банкоматами. Проаналізовано сучасні тенденції розвитку шахрайства в умовах функціонування електронного банкінгу на вітчизняному фінансовому ринку.

Ключові слова: ризик шахрайства, електронний банкінг, шахрайство з платіжними картками, шахрайство з банкоматами, фішинг.

Доминова И.В. Риск мошенничества в условиях функционирования электронного банкинга. В статье рассмотрены сущность и объекты риска мошенничества в условиях функционирования электронного банкинга. Выявлены основные источники риска мошенничества при электронном банковском обслуживании. Описаны наиболее распространенные виды мошенничества с платежными картами. Рассмотрены виды мошенничества с мобильным телефоном, Интернетом и банкоматами. Проанализированы современные тенденции развития мошенничества в условиях функционирования электронного банкинга на отечественном финансовом рынке.

Ключевые слова: риск мошенничества, электронный банкинг, мошенничество с платежными картами, мошенничество с банкоматами, фишинг.

Dominova I.V. The fraud risk under conditions of electronic banking. The article deals with the essence and objects of fraud risk in the conditions of electronic banking. The main sources of fraud risk with electronic banking services are revealed. The most common types of payment card fraud are described. Considered types of fraud with mobile phone, Internet and ATMs. Current trends in the development of fraud in the conditions of the functioning of electronic banking in the domestic financial market are analyzed.

Key words: fraud risk, electronic banking, payment card fraud, ATM fraud, phishing.

Постановка проблеми. Упровадження різних форм електронного банкінгу позитивно відобразилося на банківському обслуговуванні, зробивши його більш ефективнішим та економічно вигідним. Однак негативним є те, що банківські установи та їхні клієнти стали ще більш вразливими до шахрайських дій третіх осіб. Розповсюдження комп'ютерних вірусів, шахрайство з платіжними картками, незаконне зняття коштів з банківських рахунків, викрадення приватної, конфіденційної інформації і порушення роботи банківських автоматизованих систем обслуговування – це не повний перелік злочинів, що мають місце в електронному банківському обслуговуванні як у світі, так і в Україні.

Згідно з даними Американської асоціації банкірів, у світі здійснюється понад 2,5 трлн. операцій за кредитними картками у рік. Картки приймаються у понад 24 млн. точок у близько 200 країнах. Щосекунди здійснюється приблизно 10 тис. операцій за допомогою банківських карток [1]. Саме тому у багатьох країнах світу шахрайство через системи електронного банкінгу є небезпекою номер один. І як результат, ідентифікація та оцінка ризику шахрайства в умовах функціонування електронного банкінгу є одним із пріоритетних завдань для банківських установ, які використовують інформаційні технології у процесі банківського обслуговування.

Аналіз останніх досліджень і публікацій. Питанню безпеки банківської діяльності та протидії шахрайства приділяють увагу багато вітчизняних та зарубіжних науковців, як економістів, так і юристів, оскільки будь-який вид шахрайства (викрадення конфіденційних даних банку, фінансових ресурсів банку чи клієнта) пов'язаний з кримінальною відповідальністю. Так, серед вітчизняних науковців слід назвати таких, як М.І. Зубок, С.М. Яременко, В.М. Бутузов, В.Д. Гавловський, К.В. Тітуніна В.П. Шелеменцев, А.І. Марущак, Л.М. Стрельбицька, М.П. Стрельбицький. Відзначимо, що в основному вітчизняні науковці приділяють уваги шахрайству з платіжними картками та наголошують на необхідності захисту комп'ютерних технологій і систем банку від злочинних посягань та несанкціонованого доступу, однак відсутні дослідження у сфері безпеки обслуговування клієнтів через системи електронного банкінгу (через банкомати, Інтернет-банкінг, мобільний банкінг та тощо). Серед зарубіжних учених ризику шахрайства в умовах електронного банкінгу приділяють увагу П.В. Ревенков та Л.В. Лямін. У своїх дослідженнях ці науковці особливо приділяють увагу шахрайству через системи Інтернет-банкінгу та оцінюють вплив DDoS-атак на інформаційну безпеку банку [2, с. 69]. Натомість не приділяють уваги шахрайству з

платіжними картками та через банкомати. На інформаційну безпеку в умовах електронного банкінгу наголошує й зарубіжний дослідник Бретт Кінг, відзначаючи, що шахрайство персональних даних клієнтів (інформація про банківські рахунки, номери кредитних карток) є однією з головних проблем обслуговування клієнтів через електронні канали [3].

Формулювання цілей статті. На основі викладеного можна сформулювати завдання дослідження, яке полягає в аналізі шахрайства через системи електронного банкінгу в Україні та виявленні основних джерел їх прояву.

Виклад основного матеріалу. Видозміна процесу банківського обслуговування зумовило появу і нових видів загроз. М.І. Зубок наголошує, що найсуттєвішою загрозою як зовнішнього, так і внутрішнього походження для безпеки банку є шахрайство, відзначаючи, що предметом шахрайських посягань в умовах традиційного банківського обслуговування насамперед є гроші (75%), потім товарно-матеріальні цінності (20%), а 5% шахрайства припадає на викрадення інтелектуальної розробки банку [4, с. 68]. Натомість в умовах функціонування електронного банкінгу основними об'єктами шахрайства є:

1) конфіденційна інформація про клієнтів банківської установи (номери платіжних карток, пін-коди, CVV-код);

2) логіни та паролі доступу до систем електронного банківського обслуговування (Інтернет-банкінг та мобільний банкінг);

3) фінансові ресурси банку та клієнтів банку – доступ до яких можливий за умов викрадення вищевказаних об'єктів шахрайства.

Але основним об'єктом шахрайства є фінансові ресурси.

Сьогодні основними джерелами ризику шахрайства електронного банкінгу є операції, пов'язані з платіжними картками, обслуговування через банкомати, обслуговування в системі Інтернет-банкінгу, а також використання мобільних додатків для обслуговування через систему мобільного банкінгу. Тому, на нашу думку, для якісної ідентифікації ризику шахрайства електронного банкінгу, його варто поділяти на 1) ризик шахрайства з платіжними картками; 2) ризик шахрайства з банкоматами; 3) ризик шахрайства з мобільним телефоном та Інтернетом (рис. 1).

Насамперед відзначимо, що під ризиком шахрайства в умовах функціонування електронного банкінгу варто розуміти ймовірність втрат банківською установою або його клієнтом фінансових ресурсів за умов незаконного доступу до них третіх осіб через різні системи електронного банківського обслуговування.

Вважаємо за потрібне розглянути кожен із видів шахрайства для розуміння їх сутності та особливостей, якими вони характеризуються, що дасть змогу у подальшому їх вчасно ідентифікувати та розробити методи щодо їх попередження.

Шахрайство з платіжними картками є найпоширенішим видом шахрайства, що характеризується широким різновидом і кожного року видозмінюються. Сьогодні виокремлюють до 10 видів шахрайства із платіжними картками, однак найбільш поширенішими є соціальна інженерія (вішинг, фішинг), фармінг, трешінг.

У загальному розумінні соціальна інженерія – це метод управління діями, поведінкою людини з метою отримання від неї конкретної інформації або здійснення

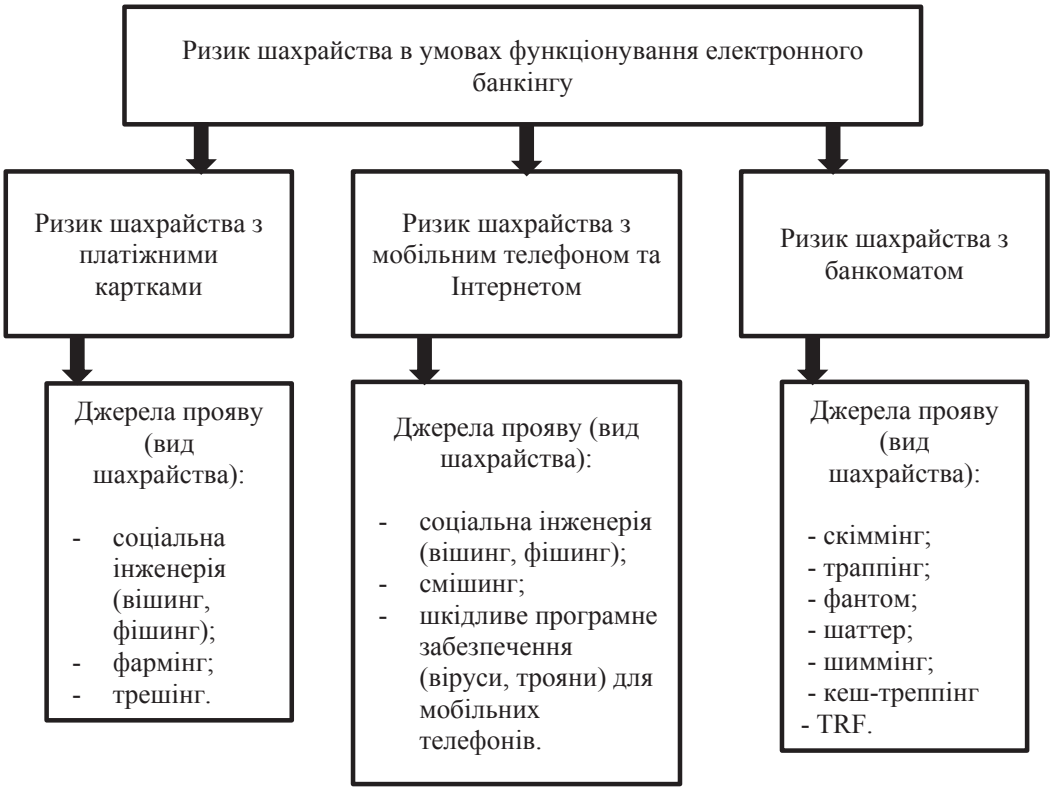

Рис. 1. Класифікація ризику шахрайства електронного банкінгу

Джерело: сформовано автором

певних дій. Цей термін використається в соціології, однак популяризація цього терміну у сфері інформаційної безпеки банку відбулася на початку XXI століття консультантом із безпеки К. Мітніком, який стверджує, що найуразливішим місцем будь-якої системи безпеки є людський фактор [5]. З цією думкою погоджується і вітчизняний науковець у сфері безпеки банківського бізнесу М.І. Зубок, який підкреслює необхідність якісного підбору персоналу для уникнення кадрового ризику, одним із проявів якого є шахрайство або розкриття конфіденційної інформації працівником банку [4, с. 374].

Методи соціальної інженерії використовують як у позитивному, так і у негативному напрямі. Проявом її негативного використання є шахрайство за допомогою методів фішингу та вішингу, які стали найбільш популярними методами шахрайства з платіжними картками не тільки в Україні, але й в усьому світі. Цей вид шахрайства в основному спрямований на неуважних або довірливих користувачів банківськими картками.

Фішинг (від fishing – рибальство) – один із шахрайських способів отримання персональної інформації (паролів, номерів карт, соціального забезпечення, банківських рахунків або кредитних карт тощо) шляхом розсилки електронних листів від імені банку, відомих брендів чи компаній, які містять посилання на підроблені сайти, що імітують роботу справжніх. У подальшому зазначена інформація використовується для ініціювання неналежних грошових переказів та поштових відправлень із-за кордону [6, с. 182]. Найчастіше шахраї підробляють сайти Інтернет-банкінгу та сайти для поповнення мобільного телефону. Коли користувач фішингового сайту вводить реквізити платіжної карти для поповнення мобільного телефону або логін та пароль для входу в систему Інтернет-банкінгу чи реквізити для переказу з карти на карту, на сторінці сайту зазначається, що відбувся збій, а цим часом власники фішингових сайтів отримують повний доступ до фінансових ресурсів власника платіжної картки.

Станом на 01.10.2017 року кількість фішингових сайтів становила 84 шт. (рис. 2), а з початку 2017 року спостерігається тенденція до їх збільшення, однак найбільш піковим роком розвитку шахрайства за допомогою фішингових сайтів був 2016 рік. Згідно з даними Української міжбанківської асоціації членів платіжних систем ЕМА, у 2016-му кожен сотий власник платіжної картки в Україні став жертвою шахраїв, а загальні втрати становили майже 340 млн. грн. [7].

Відповідно до статистичних досліджень системи міжбанківського обміну інформацією Exchange-Online, у 2016 році 95% фішингових сайтів були спрямовані на отримання реквізитів платіжних карток, пропонуючи неіснуючу послугу для переказу з картки на картку та поповнення мобільного [7].

У І кварталі 2017 року основний профіль фішингових сайтів розширився, як видно на рис. 3, фішингові сайти імітують не тільки сервіси для грошових переказів та поповнення мобільного телефону, але й сайти для покупки авіаквитків.

За даними асоціації ЄМА, за місяць роботи один фішинговий сайт відвідують від 15 до 30 тис. користувачів, що є негативним та вказує на високий рівень необізнаності користувачів платіжних карток про фішингові шахрайства.

Для боротьби з фішингом Українська міжбанківська асоціація членів платіжних систем ЕМА, яка за підтримки Державного департаменту США реалізує в Україні Національну програму сприяння безпеці електронних платежів і карткових розрахунків Safe Card, запустила проект із ліквідації шахрайських сайтів [7].

Іншим видом соціальної інженерії є підвид фішингу, що має назву «вішинг» (від англ. voice – «голос»; fishing – «рибалка») – телефонне шахрайство, пов'язане з виманюванням реквізитів банківських карток або іншої конфіденційної інформації, примушуваннями до переказу коштів на карту злодіїв [6, с. 158]. Тобто шахрай телефонує на мобільний номер жертви та представляється працівником правоохоронних органів або служби безпеки банку (у 94% випадків) чи працівником пенсійного фонду чи НБУ та змушує власника платіжної карти назвати реквізити карти для її захисту від шахрайства.

Вішинг виник у середині 2006 року, однак в Україні він набрав обертів лише в 2015 році. З цим видом шахрайства у 2015 році зіткнувся кожен 220-й українець, а 2016 році – вже кожний 80-й житель України. Внаслідок вішингу у 2016 році з рахунків українців було вкрадено 275,45 млн. грн. (або 81% від загальних втрат шахрайства з платіжними картками) проти 51,74 млн. грн. в 2015 році [8]. Середня сума вішингових операцій у 2015 році становила 834 грн., а у 2016 році – вже 1403 грн. Найчастіше жертвами вішингу стають люди пенсійного віку, а саме користувачі пенсійних проектів банківських установ, оскільки їхня необізнаність та високий рівень довіри до людей робить їх особливо вразливими до цього виду шахрайства. Відповідно до досліджень асоціації ЄМА 76% осіб, до яких телефонували шахраї, стали жертвами вішингу (надали реквізити платіжної картки) [7].

Третім різновидом шахрайства з платіжними картками є фармінг, який, як і вішинг, є різновидом фішингу. Особливістю цього виду шахрайства є те, що фармінг-технології дають змогу змінити IP-адресу сайту і під час входу на web-сторінку легітимної

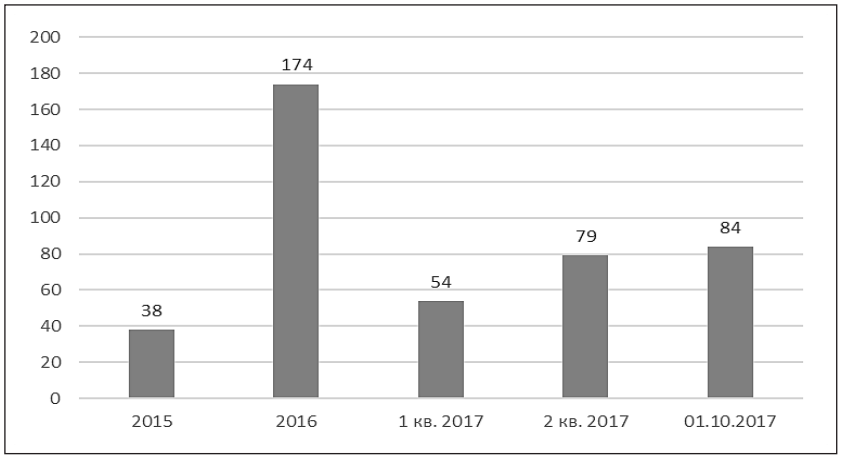

Рис. 2. Кількість виявлених фішингових сайтів у 2015–2017 рр.
Джерело: [7]

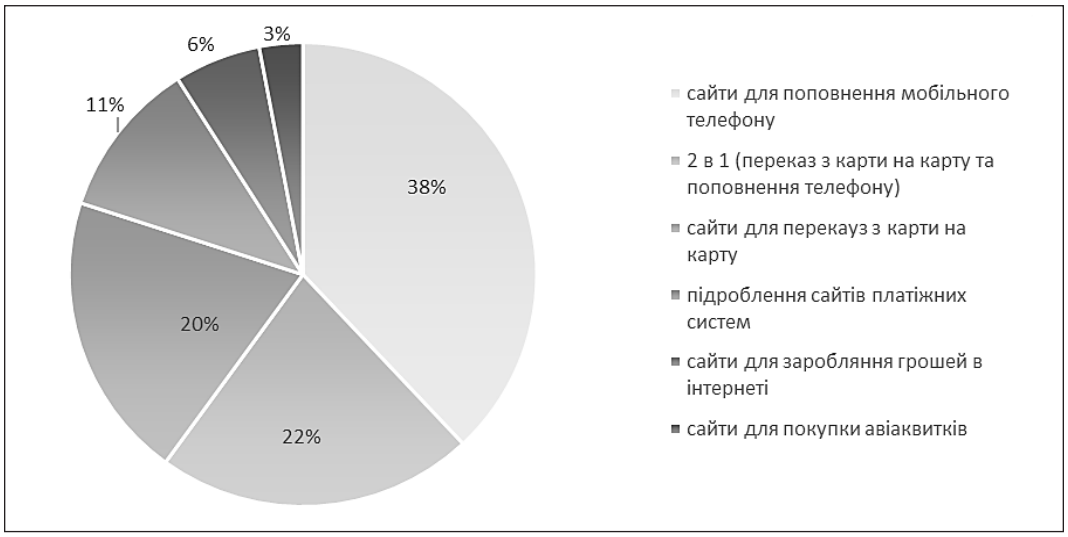

Рис. 3. Різновиди фішингових сайтів станом на 1 квартал 2017 року

Джерело: [7]

організації проводиться перенаправлення на підроблену, яка створена для збору конфіденційної інформації. Найчастіше такі сторінки підмінюють сторінки банків. Фармінг здійснюється двома способами: 1) на комп'ютер хакерами встановлюється шкідливе програмне забезпечення, яке автоматично перенаправляє користувача на нелегітимний сайт для викрадення конфіденційної інформації; 2) хакери вражають вірусами сервер DNC (сервіс доменів сайтів), у результаті чого кожен відвідувач відповідного сайту автоматично буде переправлений на сайт шахраїв. Цей вид шахрайства дуже складно розпізнати, оскільки підроблений сайт роблять фахівці своєї справи і його дуже важко розпізнати.

Варто відзначити, що під час фішингу та вішингу жертва під впливом психологічних методів та неуважності стає жертвою шахраїв, а під час фармінгу шахрай не контактує з жертвою. Найпростішим методом захисту від фармінгу є встановлення на персональний комп'ютер офіційного антивірусу.

Останнім методом шахрайства з платіжними картками є трешинг. Трешинг – це найбільш нестандартний метод отримання реквізитів карткових рахунків, оскільки шахраї шукають конфіденційну інформацію у канцелярному смітті та перепродують її третім особам, для яких ця інформація є вагомою. Цей вид шахрайства та обсяги втрат від нього важко оцінити, оскільки неможливо підрахувати та оцінити обсяги конфіденційної інформації, яка стає відкритою після потрапляння до сміттєвих баків.

Ще одна підгрупа шахрайства – це шахрайство з мобільним телефоном та Інтернетом, тобто в цю групу віднесено всі види шахрайства, для реалізації яких використовується мобільний телефон та мережа Інтернет. Такі види шахрайства, як фішинг та вішинг, також варто відносити до цієї категорії, оскільки для їх реалізації (отримання реквізитів платіжної картки) потрібне використання мобільного телефону (вішинг) або/та підключення до мережі Інтернет (фішинг).

Одним із видів шахрайства за допомогою телефону та Інтернету є смішинг – один із видів фішингу. Шахраї надсилають жертві SMS-повідомлення для мотивації жертви для переходу на фішинговий сайт або на відправку у відповідь на SMS-повідомлення реквізитів платіжної картки.

У 2017 році проявом смішингу була масова розсилка SMS-повідомлень від імені «Ощадбанку» як існуючим, так і неіснуючим клієнтам банку. На мобільні телефони приходили SMS-повідомлення з текстом «Вашу картку заблоковано». Для уточнення інформації громадянам запропонували зв'язатися з банком по двох телефонах: (099) 168-85-31 та (044) 221-35-91. Аналогічні SMS-повідомлення отримували і клієнти «ПриватБанку». Така розсилка здійснюється масово та розрахована на неуважних, необізнаних та фінансово неграмотних держателів платіжних карток.

Цей вид шахрайства спочатку здійснювався за допомогою смішингу (SMS-розсилка), а коли жертва телефонувала на вказані телефони для перевірки інформації, шахраї використовували метод вішингу (виманювання реквізитів платіжної картки за допомогою телефонної розмови). Тобто часто шахраї використовують не один метод, а їх комбінацію.

Також у цю групу відносять метод шахрайства, спрямований для отримання доступу до мобільного банкінгу чи Інтернет-банкінгу власника смартфону шляхом встановлення на нього шкідливого програмного забезпечення – «банківських троянів». Банківські трояни (Trojan-Banker) створені для викрадення облікових даних систем Інтернет-банкінгу та мобільного банкінгу, систем електронних платежів і кредитних або дебетових карт [9].

Європейські та американські банки, а також платіжні системи пропонують різні способи захисту фінансових операцій користувачів, у тому числі перевірку справжності користувача з використанням USB-токенів, одноразових паролів, підтвердження операцій за допомогою кодів, що відправляються на телефон. Проте кіберзлочинці розробляють програми, які дають змогу обходити ці захисні заходи.

Як відомо, смартфони працюють на одній із трьох платформ – iOS, Android и Windows Phone. Найбільш

поширеною платформою є Android, її частка на ринку становить 70%. За інформацією «Лабораторії Касперського», 99% шкідливого програмного забезпечення для мобільних телефонів націлені саме на платформу Android, і в середньому кожного року створюється понад 35 тис. шкідливих програм, які спрямовані на викрадення приватної інформації власника смартфону, в тому числі і паролів для входу в систему Інтернет-банкінгу чи мобільного банкінгу [9].

Протягом останнього року найпопулярнішим мобільним банківським троянцем є Trojan-Banker. AndroidOS. Svpeng.q, основною метою якого є крадіжка грошей (для отримання відомостей про банківську карту й інформації для автентифікації в онлайн-банкінгу троянець використовує фішингові вікна. Крім того, він краде гроші за допомогою SMS-сервісів, в тому числі мобільного банкінгу). Орієнтований він переважно на російськомовних користувачів.

ТОП-10 країн за часткою користувачів, які були атаковані мобільним «банківським троянцями» представлена в табл. 1

Частка атакованих українських користувачів є незначною і в другому кварталі 2017 року скоротилася, однак Україна все ще входить в десятку країн, жителі якої найчастіше атаковані шкідливими програмами для смартфонів.

Остання група, яка провокує появу ризику шахрайства в умовах функціонування електронного банкінгу, є шахрайство через банкомати. Обсяг шахрайства через банкомати в Україні йде на спад, однак залишається вагомим. Основні види шахрайства через банкомат представлені в табл. 2.

Таблиця 1

ТОП-10 країн за часткою користувачів, які були атаковані мобільним «банківським троянцями»

Країна	Частка атакованих користувачів, % 3 кв. 2016 року	Країна	Частка атакованих користувачів, % 2 кв. 2017 року
Росія	3,12	Росія	1,63
Австралія	1,42	Австралія	0,81
Україна	0,95	Туреччина	0,81
Узбекистан	0,60	Таджикистан	0,44
Таджикистан	0,56	Узбекистан	0,44
Казахстан	0,51	Україна	0,41
Китай	0,49	Латвія	0,38
Латвія	0,47	Киргизстан	0,34
Корея	0,41	Молдавія	0,34
Білорусія	0,37	Казахстан	0,32

Джерело: сформовано автором на основі [9]

Таблиця 2

Основні види шахрайства через банкомати

№	Вид шахрайства	Характеристика
1.	Скіммінг	Вид шахрайства для отримання реквізитів платіжної картки, що здійснюється за допомогою спеціального засобу, який встановлюється на банкомат,– скімера, який зчитує номер та пін-код картки. Після отримання необхідної інформації картка дублюється і гроші міняють власника за лічені хвилини.
2.	Траппінг	Вид шахрайства через банкомат, що здійснюється за допомогою «ліванської петлі», яка виготовляється з фотоплівки та встановлюється на картрідер банкомату. Потім жертва підходить до банкомату, вставляє картку, отримує гроші, але картка не повертається.
3.	Фантом	Найбільш дорогий та технічно складний вид шахрайства з банкоматом. Його суть полягає в тому, що шахраї встановлюють муляж банкомату, який виглядає як справжній банкомат, що обладнаний спеціальними пристроями, які зчитують інформацію з картки.
4.	Шаттер	Вид шахрайства, за якого на шаттер (проріз, через який відбувається видача грошей) наклеюється сторонній пристрій, що блокує видачу купюр банкоматом власнику картки. Відбувається це за рахунок розміщення липкої стрічки на внутрішній частині пристрою, до якої і пристають купюри. Відповідно, цей пристрій не дозволяє банкомату ні забрати кошти назад, ні видати їх власнику, в результаті згодом їх забирає шахрай.
5.	Шиммінг	Один зі способів незаконного зняття грошей за допомогою використання тонкої плівочки, схожої на скоч. Така плівка наклеюється на клавіатуру банкомата, а потім із неї зчитується необхідна інформація. Незвичайна клавіатура банкомата не викликає підозри, що значно полегшує завдання злочинцям.
6.	Кеш-треппінг	Вид шахрайства, що здійснюється за допомогою закриття отвору для видачі грошей в банкоматі спеціальної накладкою (планкою) з липкою стрічкою зі зворотного боку. Таким чином, під час проведення громадянами операцій зі зняття готівки відбувається захоплення купюр (гроші прилипають до планки), що перешкоджає їх видачі законному власнику картки.
7.	TRF (Transaction Reversal Fraud – скасування операції)	Шахрайство через банкомат, що здійснюється шляхом втручання в роботу банкомату під час здійснення операцій видачі готівки, яке залишає незмінним баланс карткового рахунку за фактичного отримання готівки зловмисником.

Джерело: сформовано автором на основі [6; 10; 11]

Відповідно до опублікованих даних статистичного дослідження міжбанківської асоціації членів платіжної системи ЄМА (рис. 4) в Україні найбільш популярними видами шахрайства через банкомат є кеш-треппінг та скіммінг. Найбільша частка цих злочинів припадає на міста Київ та Одесу, що пояснюється значною концентрацією населення та туристів у цих містах.

Всі вищеописані види шахрайства спрямовані насамперед на отримання карткових реквізитів для доступу до фінансових ресурсів клієнтів. Ці види шахрайства впливають на фінансовий стан клієнтів банку, а не на сам банк.

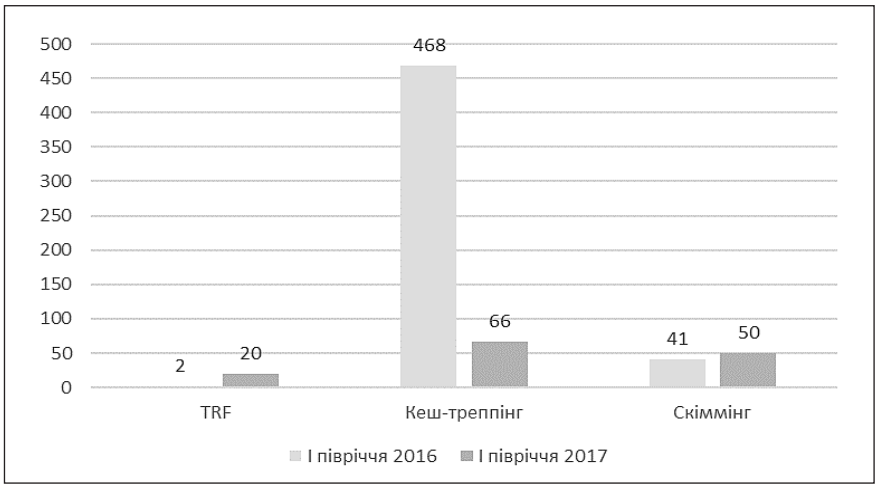

Рис. 4. Кількість інцидентів банківського шахрайства у І півріччі 2016 та 2017 років

Джерело: [7]

В Україні банківські установи повертають втрачені клієнтами кошти, оскільки переважно клієнт самостійно, однак ненавмисно розкриває свої карткові реквізити шахраям. І, як результат, банки перекладають відповідальність на клієнтів. Проте у 2016 році платіжна система VISA запровадила в Україні принцип нульової відповідальності для власників її карт, суть якого полягає в тому, що банк зобов'язаний відшкодувати власникам картки VISA викрадені шахраями кошти у разі підтвердження відсутності сприяння шахрайству з боку власника картки. Платіжні системи «Простір» та MasterCard утримались від прийняття подібних рішень, перекладаючи відповідальність на держателів платіжних карток, що за умов зростання обсягів шахрайства негативно відобразиться на репутації банківських установ.

Варто наголосити, що наслідком значної кількості шахрайства через системи електронного банкінгу є зниження довіри громадян загалом до надійності фінансової системи, банківських установ, інституту банківської таємниці, надійності захисту персональних даних, а також до фінансових операцій, що проводяться з використанням новітніх технологій. При цьому недовіра населення до ринків фінансових послуг не дає можливості активно використовувати вільні кошти громадян як інвестиційні ресурси, що спрямовуються на розвиток економіки.

Загалом такі наслідки варто розділити на такі групи: 1) фінансові – втрата коштів банківськими установами та їх клієнтами (юридичним та фізичними особами); 2) іміджеві (репутаційні) – розкриття конфіденційної інформації, у тому числі банківської таємниці та персональних даних; недовіра клієнтів до банківської системи загалом та систем ДБО зокрема, що тягне за собою зменшення обсягу безготівкових операцій; 3) юридичні – позови клієнтів; 4) технологічні – з метою забезпечення надійної роботи інформаційних, комп'ютерних та телекомунікаційних систем банківські установи, підприємства та організації змушені створювати (або придбавати) складніші, дорожчі та менш зручні у використанні засоби захисту [10, с. 14].

Висновки. Отже, в умовах функціонування електронного банкінгу ризик шахрайства є невід'ємною частиною банківського обслуговування. В основному він проявляється у викраденні конфіденційних даних клієнтів для доступу до їхніх фінансових ресурсів. Його ідентифікація здійснюється за умов якісного розподілення джерел шахрайства на три групи: ризик шахрайства з платіжними картками; ризик шахрайства з банкоматом; ризик шахрайства з мобільним телефоном та Інтернетом. Запропонований підхід дає змогу не розпорошувати увагу на велику кількість джерел, що можуть зумовити виникнення ризикових подій та вчасно ідентифікувати ризики шахрайства електронного банкінгу. Перспективою подальших наукових досліджень у цьому напрямі є проведення дослідження та розроблення методів мінімізації ризику шахрайства в умовах функціонування електронного банкінгу.

Список використаних джерел:

1. Офіційний сайт Американської асоціації банкірів [Електронний ресурс]. – Режим доступу: https://www.aba.com/Compliance/Pages/Staff-Analysis.aspx

2. Применение технологий электронного банкинга: риск-ориентированный подход /Л.В. Лямин. – М.: КНОРУС; ЦИПСиР, 2011. – 336 с.

3. Банк 3.0. Почему сегодня банк – это не то, куда вы ходите, а то, что вы делаете / Бретт Кинг // [Пер. с англ. М. Мацковской]. – М.: Издательство «Олимп–Бизнес», 2015. – 520 с.

4. Безпека банківської діяльності: підручник / М.І. Зубок, С.М. Яременко. – К.: КНЕУ, 2012. – 473 с.

5. Искусство обмана / Митник Кевин, Саймон Вильям. – АйТи, 2004. – 360 с.

6. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток: науково-практичний посібник / За редакцією І.В. Бондаренка. – К.:, 2009. – 182 с.

7. Офіційний сайт Української міжбанківської асоціації платіжної системи ЄМА [Електронний ресурс]. – Режим доступу: https://ema.com.ua/fraud-digest-25-07-2017/

8. Офіційний сайт Національного банку України [Електронний ресурс]. – Режим доступу: https://bank.gov.ua/control/uk/publish/category?cat_id=79219
9. Офіційний сайт компанії «Лабораторії Касперського» [Електронний ресурс]. – Режим доступу: https://securelist.ru/it-threat-evolution-q2-2017-statistics/79226/
10. Кіберзлочинність та відмивання коштів / Департамент фінансових розслідувань Державна служба фінансового моніторингу України. – Київ, 2013. – 53 с.
11. Пивоваров В.В. Шахрайство із банківськими картками: окремі питання віктимологічної профілактики /В.В. Пивоваров, К.В. Терещенко // Карпатський правничий часопис. – 2015. – № 10. – С. 132-137

УДК 336.227.2

Коніна М.О.,
асистент кафедри фінансів та банківської справи,
Донецький національний університет економіки та торгівлі імені Михайла Туган-Барановського
Овчаренко К.В.,
студентка,
Донецький національний університет економіки та торгівлі імені Михайла Туган-Барановського

СОЦІАЛЬНО-ЕКОНОМІЧНІ НАСЛІДКИ УХИЛЕННЯ ВІД СПЛАТИ ПОДАТКІВ

Коніна М.О., Овчаренко К.В. Соціально-економічні наслідки ухилення від сплати податків. У статті розглядається проблема ухилення від сплати податків в Україні та наслідків цього явища. Доведено втрати державного бюджету від ухилення від сплати податків. Названо форми ухилення від сплати податків, що використовуються суб'єктами господарювання. Також досліджено негативні наслідки цієї проблеми для економіки України. Запропоновано шляхи вирішення проблеми боротьби з ухиленням від сплати податків, виходячи з позитивного досвіду розвинених країн.

Ключові слова: податки, система оподаткування, тінізація економіки, фіскальний тиск, ухилення від оподаткування.

Конина М.А., Овчаренко К.В. Социально-экономические последствия уклонения от уплаты налогов. В статье рассматривается проблема уклонения от уплаты налогов в Украине и последствий этого явления. Доказаны потери государственного бюджета от уклонения от уплаты налогов. Названы формы уклонения от уплаты налогов, которые используются субъектами хозяйствования. Также исследованы негативные последствия этой проблемы для экономики Украины. Предложены пути решения проблемы борьбы с уклонением от уплаты налогов, исходя из положительного опыта развитых стран.

Ключевые слова: налоги, система налогообложения, тенизация экономики, фискальное давление, уклонение от налогообложения.

Konina M.A., Ovcharenko K.V. Socio-economic consequences of tax evasion. The article considers the problem of tax evasion in Ukraine and the consequences of this phenomenon. Proved the loss of the state budget from tax evasion. The named tax evasion forms used by economic entities. Also it is written about different negative consequences of this problem for the economy of Ukraine. The ways of solving the problem of fighting tax evasion calculation based on the positive experience of developed countries are offered.

Key words: taxes, tax system, the shadow economy, fiscal pressure, tax evasion.

Постановка проблеми. Одним із найважливіших елементів економіки кожної країни є податкова система. Українська податкова система формується в складних кризових умовах. Як наслідок, дедалі більшого значення в українській економіці набуває проблема ухилення від сплати податків. Останнім часом це навіть стало нормою поведінки великої кількості суб'єктів господарської діяльності. Ухилення від сплати податків є одним із видів економічних злочинів. Вирішення цієї проблеми є дуже важливим з огляду на протидію фінансовим злочинам і необхідність залучення коштів до державного бюджету України. Заходи боротьби з тіньовою економікою, що зараз застосовуються, не дають бажаного ефекту з різних причин, серед яких – висока здатність тіньової економіки до самовідтворення.

Аналіз останніх досліджень та публікацій. Щодо проблеми ухилення від сплати податків, зборів та інших обов'язкових платежів довгий час дискутують багато вчених-юристів, економістів і нау-