ШАХРАЙСТВА ЕЛЕКТРОННОГО БАНКІНГУ: ІДЕНТИФІКАЦІЯ ТА ЗАПОБІГАННЯ РИЗИКАМ

ELECTRONIC BANKING FRAUD: IDENTIFICATION AND RISK PREVENTION

УДК 336.71:004.771
DOI: https://doi.org/10.32843/bses.48-87

Тришак Л.С.
к.е.н., доцент,
доцент кафедри фінансів
Івано-Франківський національний
технічний університет нафти і газу
Орищин Т.М.
к.е.н., доцент,
доцент кафедри фінансів
Івано-Франківський національний
технічний університет нафти і газу

Tryshak Lidiia
Ivano-Frankivsk National
Technical University of Oil and Gas
Oryshchyn Tetiana
Ivano-Frankivsk National
Technical University of Oil and Gas

Стаття присвячена дослідженню основних засад ідентифікації шахрайств та оцінювання ризиків електронного банкінгу, розробленню рекомендацій щодо мінімізації ризиків електронного банкінгу та контролю за цими ризиками. Узагальнено та систематизовано наукові підходи до визначення поняття «електронний банкінг», обґрунтовано відмінність між електронним банкінгом та дистанційним банківським обслуговуванням і встановлено, що дистанційне банківське обслуговування є одним зі способів здійснення електронного банківського обслуговування. Застосування отриманих у роботі результатів дослідження забезпечує підвищення точності і якості ідентифікації та оцінювання ризиків шахрайств електронного банкінгу. Запропоновані у процесі дослідження підходи до мінімізації ризиків електронного банкінгу та напрями вдосконалення внутрішньобанківських систем управління ризиками електронного банкінгу дають змогу підвищити ефективність управління цими ризиками.
Ключові слова: *електронний банкінг, ризики електронного банкінгу, форми електронного банкінгу, дистанційний банкінг, шахрайства електронного банкінгу.*

Статья посвящена исследованию основных принципов идентификации мошенничества и оценки рисков электронного банкинга, разработке рекомендаций по минимизации рисков электронного банкинга и контроля за этими рисками. Обобщены и систематизированы научные подходы к определению понятия «электронный банкинг», обосновано различие между электронным банкингом и дистанционным банковским обслуживанием и установлено, что дистанционное банковское обслуживание является одним из способов осуществления электронного банковского обслуживания. Применение полученных в работе результатов исследования обеспечивает повышение точности и качества идентификации и оценки рисков мошенничества электронного банкинга. Предложенные в процессе исследования подходы к минимизации рисков мошенничества электронного банкинга и направления совершенствования внутрибанковских систем управления рисками электронного банкинга позволяют повысить эффективность управления этими рисками.
Ключевые слова: *электронный банкинг, риски электронного банкинга, формы электронного банкинга, дистанционный банкинг, мошенничества электронного банкинга.*

The article presents an in-depth study of the theoretical and methodological principles of identification and assessment of risks in electronic banking; and also presents recommendations on how to minimize the risks of electronic banking and manage these risks effectively. Includes: generalized and systematized scientific approaches to the definition of the concept of "electronic banking;" identification of signs and risks of electronic banking. The study suggests defining electronic banking as an innovative way of banking services that allows providing traditional services, as well as information services, through various types of electronic banking, each of which can be modified and improved under the development of information technologies. The work defines the primary distinction between electronic and remote banking and confirms that remote banking can serve as a type of maintaining electronic banking. The basic types of electronic banking fraud are considered. Proved that the primary sources of electronic banking fraud risks are transactions related to bank cards as they contain vital information (CVV-code, expiration date, and card number) with which bank customer's financial resources can be the bank's financial resources can be stolen. E-banking services are characterized by specific features that predetermine expansion of banking risk sources. These features include 1) remoteness of a client from the banking institution; 2) in the process of carrying out banking operations, it is a client, not a qualified employee of a bank, who acts as a teller (client-teller); 3) the level of service quality depends on the e-banking services operation entirely. It has been proven that similar risks are inherent in various types of electronic banking. The application of the results obtained during the research can increase the accuracy and quality of identification and assessment of the possible risks of electronic banking. Furthermore, approaches to minimizing the risks of electronic banking and ways of improving the intrabank systems of electronic banking risk management, which were proposed and developed in the research process, allow increasing the effectiveness of managing the risks.
Key words: *electronic banking, electronic banking risks, forms of electronic banking, remote banking, electronic banking fraud.*

Постановка проблеми. Функціонування банківських установ на сучасному етапі розвитку економіки спонукає їх до використання інноваційних технологій банківського обслуговування, які дають можливість зайняти провідні конкурентні позиції на ринку. Упровадження різних форм електронного банкінгу підвищило ефективність обслуговування клієнтів та зробило його економічно вигідним, проте такі види діяльності банків стали особливо вразливими до шахрайських дій злочинців. В електронному банківському обслуговуванні клієнтів все частіше застосовуються такі види злочинів, як шахрайство із платіжними картками, розповсюдження комп'ютерних вірусів, незаконне зняття коштів із банківських рахунків, викрадення конфіденційної інформації тощо. За таких умов дослідження видів основних шахрайств електронного банкінгу та методів мінімізації ризиків, пов'язаних із таким видом банківського обслуговування клієнтів, набувають важливого значення та актуальності.

Аналіз останніх досліджень і публікацій. Теоретичні засади сутності та форм електронного банкінгу, видів шахрайств, а також методи управління ризиками електронної форми обслуговування клієнтів банків досліджували такі вчені, як О. Вовчак, Б. Кінг, М. Зубко, І. Домінова, Г. Шпаргало, Л. Капінус, І. Пасічник, Г. Карчева, В. Бутузов та інші.

Постановка завдання. Метою дослідження є узагальнення основних теоретичних засад ідентифікації шахрайств електронного банкінгу та розроблення рекомендацій щодо запобігання банківськими установами ризиків, пов'язаних із таким видом обслуговування клієнтів.

Виклад основного матеріалу дослідження. Електронний банкінг набуває неймовірної популярності, тому дослідження специфіки цієї форми банківського обслуговування клієнтів має особливе значення. За електронної форми обслуговування клієнтів небезпекою номер один є шахрайства та кіберзлочини, а тому для банківських установ, які використовують інформаційні технології у процесі банківського обслуговування клієнтів, одним із пріоритетних завдань є ідентифікація та оцінювання загроз шахрайства електронного банкінгу.

Дослідження визначень сутності електронного банкінгу у науковій літературі за змістом не збігаються. Так, вітчизняні науковці О. Вовчак та Г. Шпаргало розглядають електронний банкінг як діяльність банку з надання комплексу послуг клієнтам за допомогою комп'ютерних технологій. На їхню думку, під електронними банківськими послугами слід розуміти дії банку, спрямовані на вдосконалення та реалізацію звичних банківських операцій шляхом використання інформаційних систем [1].

І. Пасічник та К. Базадзе ототожнюють електронний банкінг та електронну банківську діяльність як синонімічні поняття і визначають його як «процес здійснення банківських операцій та надання банківських послуг із використанням автоматизованих систем, у тому числі електронних каналів зв'язку» [2].

Поняття електронного банкінгу досліджують Л. Капінус і Н. Скригун, інтерпретуючи його як послугу банку, що передбачає дистанційне керування рухом фінансових коштів на картковому рахунку за допомогою електронних мереж і обладнання [3]. А. Новицький наводить подібне визначення електронного банкінгу, проте наголошує, що електронне банківське обслуговування є спеціальним інструментом для надання банківських послуг на відстані за допомогою телекомунікаційних та новітніх інформаційних технологій [4, с. 209].

Часто в науковій економічній літературі використовується таке визначення електронного банкінгу, як «забезпечення можливостей для клієнтів банків отримувати віддалений доступ до своїх банківських рахунків через інформаційно-телекомунікаційні системи та, як мінімум, здійснювати перекази фінансових коштів між ними» [5, с. 121].

Чіткого визначення економічного змісту електронного банкінгу також немає серед зарубіжних науковців. Більшість зарубіжних учених описують електронний банкінг як електронний зв'язок (через комп'ютер або мобільний телефон) між банком і клієнтом для підготовки, управління та контролю за проведенням фінансових операцій і послуг [6]. Часто поняття електронного банкінгу вживають як узагальнене визначення для дослідження особливостей дистанційного електронного обслуговування клієнтів банку.

Слід зазначити, що у вітчизняному банківському законодавстві, в тому числі у Законі України «Про банки та банківську діяльність», не наведено визначення «електронне банківське обслуговування» або «електронний банкінг». Першим кроком до законодавчого регулювання електронного банкінгу стало прийняття Закону України «Про електронний цифровий підпис», Закону України «Про електронні документи та електронний документообіг», а також лист Департаменту платіжних систем Національного банку України «Про надання інформації про використання Інтернет-технологій клієнтами банків при здійсненні розрахунків», у якому згадується про одну із форм електронного банкінгу – Інтернет-банкінг.

Визначення електронного банкінгу наводить Базельський комітет із банківського нагляду: «електронний банкінг – це надання роздрібних і незначних за обсягом банківських продуктів та послуг через електронні банківські канали, а також значних за обсягом електронних платежів та інших оптових банківських послуг електронним шляхом» [7].

Наведені визначення дають підстави зробити висновок, що немає єдиного підходу до розуміння електронного банкінгу серед науковців та практиків банківської справи. За сутнісним змістом більшість науковців вважають, що під електронним банкінгом варто розуміти вид дистанційного банківського обслуговування, через який здійснюється процес надання банківських послуг лише за допомогою використання Інтернету та мобільного зв'язку. Проте вважаємо, що «електронний банкінг» і «дистанційне банківське обслуговування» не є синонімічними поняттями.

Так, електронне банківське обслуговування клієнтів не завжди здійснюється дистанційно, адже обслуговування через термінали самообслуговування та банкомати зазвичай відбувається у відділеннях банківських установ, а дистанційне банківське обслуговування відбувається лише тоді, коли клієнт не обслуговується у відділенні. Отже, поняття «електронний банкінг» є ширшим за поняття «дистанційне банківське обслуговування». Спільним між електронним банкінгом і дистанційним обслуговуванням є те, що клієнт сам виступає операціоністом під час використання цих способів банківського обслуговування.

З огляду на наведені вище визначення електронного банкінгу та специфічні характерні ознаки цього способу обслуговування клієнтів вважаємо, що під поняттям «електронний банкінг» слід розуміти спосіб банківського обслуговування, за допомогою якого надаються традиційні та інформаційні послуги банківського обслуговування через різні автоматизовані форми інформаційних технологій.

В умовах функціонування та розвитку форм електронного банкінгу збільшується загроза кіберзлочинності та шахрайств. Багато вітчизняних та

зарубіжних науковців приділяють увагу дослідженню питання безпеки банківської діяльності та протидії шахрайствам електронного банкінгу. Так, вітчизняні науковці М.І. Зубок та С.М. Яременко доводять, що безпека банківської діяльності – це стан стійкої життєдіяльності, за якого забезпечується реалізація мети банку та основних його інтересів, захист від внутрішніх та зовнішніх дестабілізувальних факторів незалежно від умов функціонування. Вважається, що найсуттєвішою загрозою як зовнішнього, так і внутрішнього походження для безпеки банку є ризик шахрайства, відзначаючи, що предметом шахрайських посягань насамперед є гроші (75%), товарно-матеріальні цінності (20%), а 5% шахрайств припадає на викрадення інтелектуальної розробки банку [8].

В.М. Бутузов та В.Д. Гавловський зазначають, що предметом злочину у сфері використання платіжних карток є: 1) інформація, що дає змогу ініціювати переказ коштів; 2) кошти на картковому рахунку держателя платіжної картки; 3) майно та послуги торговельних та сервісних підприємств, що здійснюють карткові розрахунки [9].

На інформаційній безпеці в умовах електронного банкінгу наголошує й зарубіжний дослідник Бретт Кінг, відзначаючи, що шахрайство з персональними даними клієнтів є однією з головних проблем обслуговування клієнтів через електронні канали [10].

Базельський комітет із питань банківського нагляду теж наголошує на необхідності ідентифікації шахрайства електронного банкінгу та мінімізації ризику цієї форми банківського обслуговування клієнтів. Так, у Базелі III вказано, що ризик шахрайства є складником операційного ризику електронного банкінгу, та зазначено, що внутрішнє і зовнішнє шахрайство у банку описується як події, що пов'язані з операційним ризиком банку [11]. Тобто у цьому разі шахрайство є не окремим підвидом ризику, а загрозою – потенційними чи реальними діями певних суб'єктів, що здатні завдати конкретному банку матеріальної або моральної шкоди [8]. Особливістю загроз є те, що вони є конкретними і призводять до фінансових втрат банків та їхніх клієнтів.

Узагальнюючи зазначене, можна визначити такі основні об'єкти шахрайства електронного банкінгу, як: 1) конфіденційна інформація про клієнтів банку (пін-коди, CVV-код); 2) логіни та паролі доступу до форм електронного банкінгу (Інтернет-банкінг та мобільний банкінг); 3) фінансові ресурси банку та клієнтів банку, доступ до яких можливий за умов викрадення вищевказаних об'єктів шахрайства [12, с. 93].

Отже, можемо констатувати, що не досить уваги приділяється процесу ідентифікації та оцінювання ризику шахрайства електронного банкінгу, що ускладнює подальший процес дослідження. Ідентифікація шахрайства електронного банкінгу пов'язана з виявленням джерел, які провокують появу ризику, притаманного цьому виду банківської діяльності.

Нині найбільшими ризиками шахрайств електронного банкінгу є: 1) шахрайства з платіжними картками; 2) шахрайства через мобільний телефон та Інтернет.

З метою ідентифікації джерел прояву ризиків шахрайств, притаманних кожній із наведених форм функціонування електронного банкінгу, проаналізуємо їх види.

Так, шахрайства з платіжними картками, з мобільним телефоном та Інтернетом переважно здійснюються за допомогою таких методів, як соціальна інженерія (до яких належить фішинг, вішинг), фармінг, трешінг, основною метою яких є отримання конфіденційної інформації, що вказана на платіжній картці. Шахрайства з платіжними картками є найпоширенішим видом шахрайства в Україні.

Для розуміння сутності шахрайства електронного банкінгу та специфіки ризиків, якими він характеризується, розглянемо детальніше кожен із його видів, що дасть змогу надалі вчасно їх ідентифікувати та розробити методи запобігання цим ризикам.

Соціальна інженерія – це метод управління діями і поведінкою людини з метою отримання від неї певної інформації або здійснення певних дій. Так, М.І. Зубок підкреслює необхідність якісного підбору персоналу для уникнення кадрового ризику, одним із проявів якого є шахрайство або розкриття конфіденційної інформації працівником банку [8, с. 374].

Найбільш популярними видами шахрайства з платіжними картками з використанням методів соціальної інженерії є фішинг та вішинг, які спрямовані на неуважних або довірливих користувачів банківськими платіжними картками.

Фішинг (від fishing – рибальство) – спосіб отримання персональної інформації (номерів карт, паролів, банківських рахунків) шляхом розсилки електронних листів від імені банку чи відомих компаній, які містять посилання на підроблені сайти, що емітують роботу справжніх. У подальшому зазначена інформація використовується для ініціювання з-за кордону неналежних грошових переказів та поштових відправлень [12, с. 94]. Техніка фішингу була описана ще в 1987 році, проте термін phishing почали використовувати у 1996 році у США у зв'язку з активним розвитком цього виду шахрайства.

Наступним видом шахрайства є вішинг (від англ. voice – «голос» – телефонне шахрайство, пов'язане з видурюванням конфіденційної інформації щодо реквізитів банківських карток та їх паролів і схиляннням до переказу коштів на картку злодіїв (шахрай телефонує потенційній жертві шахрайства та представляється працівником правоохоронних органів або служби безпеки банку

(у 94% випадків) та змушує власника платіжної картки назвати її реквізити) [12, с. 94].

Наступний різновид шахрайства з платіжними картками – це фармінг. Змістом цього виду шахрайства є те, що фармінг-технології дають змогу змінити IP-адрес сайту, і під час входу на web-сторінку легітимної організації проводиться перенаправлення на підроблену, яка створена для збору конфіденційної інформації [12, с. 94].

Слід зазначити, що під впливом психологічних методів чи неуважності людина стає жертвою шахраїв, якщо йдеться про фішинг та вішинг, тоді як під час фармінгу шахрай не контактує з жертвою, а тому захистом від фармінгу може бути встановлення на персональний комп'ютер ліцензійного антивірусу.

Наступна підгрупа шахрайств електронного банкінгу – це шахрайства з мобільним телефоном та Інтернетом. У цю групу віднесено всі види шахрайства, для реалізації яких використовується мобільний телефон та мережа Інтернет. Так, різновидом шахрайства за допомогою телефону та Інтернету є смішинг, коли шахраї надсилають жертві SMS-повідомлення для переходу на фішинговий сайт або для відправлення у відповідь на SMS-повідомлення реквізитів платіжної картки [12, с. 95].

Всі описані види шахрайства електронного банкінгу націлені на доступ до фінансових ресурсів клієнтів через отримання конфіденційної інформації щодо їхніх карткових реквізитів та негативно впливають як на фінансовий стан клієнтів банку, так і на репутацію банківської установи.

Зниження довіри громадян до вітчизняної банківської системи загалом та надійності банківських установ зокрема, а також до захисту їхніх персональних даних є наслідком значної кількості шахрайства через системи електронного банкінгу. При цьому така недовіра населення до банківських установ знижує можливість банків спрямовувати вільні кошти громадян у вигляді інвестиційних ресурсів на розвиток економіки України.

Висновки з проведеного дослідження. Підсумовуючи викладене, слід зазначити, що обслуговування банками клієнтів із використанням різних форм електронного банкінгу пов'язане з різними видами шахрайства, а тому з боку банківських установ потребує управління ризиками, які притаманні такому виду банківського бізнесу.

З метою запобігання ризикам шахрайств, що виникають під час електронного обслуговування клієнтів, банківські установи повинні будувати чітку систему їх ідентифікації та мінімізації. До основних методів мінімізації ризиків шахрайства електронного банкінгу можна віднести:

1) підвищення фінансової грамотності клієнтів через їхню обізнаність щодо видів шахрайств електронного банкінгу з метою скорочення їхніх фінансових втрат від шахрайства. Цього можна досягти такими способами, як:

– надання банківським працівником у вигляді флаєра чи брошури повної інформації щодо видів шахрайств із платіжними картками під час отримання клієнтом банківської картки;

– надсилання на електронну пошту клієнтів листів про нові форми шахрайств електронного банкінгу;

– поширення банками інформації про види шахрайства електронного банкінгу через засоби масової інформації та соціальні мережі;

– інформування банками своїх клієнтів щодо порядку дій у разі втрати або викрадення карти з метою вчасного блокування їхніх рахунків.

2) модернізація та захист власних програмних комплексів банків відповідно до сучасних вимог безпеки, а також проведення постійного моніторингу ринку електронного банківського обслуговування з метою виявлення нових видів шахрайства.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Вовчак О.Д., Шпаргало Т.Я. Андрейків Г.Є. Платіжні системи. Київ : Знання, 2008. 341 с.

2. Пасічник І.В., Базадзе К.М. Підвищення конкурентоспроможності банківських установ на основі використання електронних технологій. *Фінансово-кредитна діяльність : проблеми теорії та практики.* 2011. № 1(10). С. 217–223.

3. Капінус Л.В., Скригун Н.П. Development of electronic banking technologies in Ukraine. *Економічний часопис-XXI.* 2014. № 3-4(1). С. 55–58.

4. Новицький А.М. Правове регулювання інституціоналізації інформаційного суспільства в Україні. Ірпінь : НУ ДПС України, 2011. 444 с.

5. Карчева Г.Т. Теоретичні та практичні аспекти управління ризиками електронного банкінгу. *Науковий вісник Полісся.* 2015. № 2(2). С. 121–126.

6. Shraddha Nigudge, Mohsin Khan A. Pathan E-banking : Services, Importance in Business, Advantages, Challenges and Adoption in India. *Asian Journal of Management Sciences.* 2014. № 02(03 (Special Issue)). p. 190–192.

7. Risk Management for Electronic Banking and Electronic Money Activities. Basel : Basel Committee on Banking Supervision, Mart 1998.

8. Зубок М.І., Яременко С.М. Безпека банківської діяльності : підручник. Київ : КНЕУ, 2012. 473 с.

9. Правові та організаційні засади протидії злочинам у сфері платіжних карток : науково-практичний посібник / В.М. Бутузов та ін. ; за ред. І.В. Бондаренка. Київ, 2009. 182 с.

10. Кинг Б. Банк 3.0 : Почему сегодня банк – это не то, куда вы ходите, а то, что вы делаете / пер. с англ. М. Мацковской. Москва : ЗАО «Олимп-Бизнес», 2014. 520 с.

11. Basel III : A global regulatory framework for more résilient banks and banking systems. Basel : Basel Committee on Banking Supervision, June 2011.

12. Домінова І.В. Ризик шахрайства в умовах функціонування електронного банкінгу. *Науково-виробничий журнал «Бізнес- навігатор».* 2017. № 4-2 С. 92–98.

REFERENCES:

1. Vovchak O.D. (2008) *Platizhni systemy* [Payment systems]. Kyiv : Znannia. (in Ukrainian)

2. Pasichnyk I.V., Bazadze K.M. (2011) Pidvyshhennja konkurentospromozhnosti bankivsjkykh ustanov na osnovi vykorystannja elektronnykh tekhnologhij. [Enhancing the competitiveness of banking institutions through the use of electronic technologies]. *Finansovo-kredytna dijaljnistj : problemy teoriji ta praktyky*, no. 1(10). pp. 217–223.

3. Kapinus L.V., Skryghun N.P. (2014) Development of electronic banking technologies in Ukraine. *Ekonomichnyj chasopys – XXI*, no. 3-4(1), pp. 55–58.

4. Novycjkyj A.M. (2011) *Pravove reghuljuvannja instytucionalizaciji informacijnogho suspiljstva v Ukrajini* [Legal regulation of the institutionalization of the information societyin Ukraine]. Irpinj : NU DPS Ukrajiny (in Ukrainian)

5. Karcheva Gh.T. (2015) Teoretychni ta praktychni aspekty upravlinnja ryzykamy elektronnogho bankinghu [Teoretical and practical aspects of e-banking risk management]. *Naukovyj visnyk Polissj*, no. 2(2), pp. 121–126.

6. Shraddha Nigudge, Mohsin Khan A. Pathan E-banking : Services, Importance in Business, Advantages, Challenges and Adoption in India. *Asian Journal of Management Sciences.* 2014. № 02(03 (Special Issue)). p. 190–192.

7. Risk Management for Electronic Banking and Electronic Money Activities. Basel : Basel Committee on Banking Supervision, Mart 1998.

8. Zubok M.I., Jaremenko S.M. (2012) *Bezpeka bankivsjkoji dijaljnosti* : pidruchnyk [Security of banking activities : a textbook]. Kyjiv : KNEU. (in Ukrainian)

9. Butuzov V.M., Ghavlovsjkyj V.D., Titunina K.V., Shelomencev V.P. (2009) *Pravovi ta orghanizacijni zasady protydiji zlochynam u sferi platizhnykh kartok : naukovo-praktychnyj posibnyk* [Legal and organizational basis for counteraction to payment card crimes : scientific and practical manual]. Kyjiv. (in Ukrainian)

10. King B. (2014) *Bank 3.0 : Pochemu segodnya bank – eto ne to, kuda vy khodite, a to, chto vy delaete* [Bank 3.0: Why banking is no longer somewhere you go but something you do]. Moskva : ZAO «Olimp-Biznes» (in Russian)

11. Basel III: A global regulatory framework for more résilient banks and banking systems. Basel : Basel Committee on Banking Supervision, June 2011.

12. Dominova I.V. (2017) Ryzyk shakhrajstva v umovakh funkcionuvannja elektronnogho bankinghu [The risk of fraud in the functioning of electroning of electronic banking]. *Naukovo-vyrobnychyj zhurnal «Biznes-navighator»*, no. 4-2, pp. 92–98.