УДК 330.101
DOI: https://doi.org/10.32782/2224-6282/165-20

Годнюк І. В.
кандидат економічних наук, доцент,
Подільський спеціальний навчально-реабілітаційний
соціально-економічний коледж
ORCID: https://orcid.org/0000-0003-3346-0882

Шубенко І. А.
кандидат економічних наук, доцент,
Поліський національний університет
ORCID: https://orcid.org/0000-0002-3461-9237

Вольська А. О.
кандидат економічних наук, доцент,
Подільський спеціальний навчально-реабілітаційний
соціально-економічний коледж
ORCID: https://orcid.org/0000-0001-7119-0436

Godniuk Irina
Podilsky Special Education and Rehabilitation Socio-economic College
Shubenko Inna
Polissya National University
Volska Angeliia
Podilsky Special Education and Rehabilitation Socio-economic College

ФІНАНСОВЕ ШАХРАЙСТВО У КОМЕРЦІЙНИХ БАНКАХ УКРАЇНИ. ШЛЯХИ БОРОТЬБИ У СФЕРІ БЕЗГОТІВКОВИХ РОЗРАХУНКІВ

Однією з перешкод ефективному розвитку банківської діяльності є фінансове шахрайство, що являє собою систему відносин у сфері грошового обігу та фінансових зобов'язань, метою яких є недобросовісне заволодіння фінансовими ресурсами банків і/або їхніх клієнтів шляхом обману або зловживання довірою чи службовим становищем громадян і працівників банківських установ. До того ж недосконала правова система сприяє тому, що в державі продовжують доволі активно реалізовувати різноманітні шахрайські схеми. Забезпечення ефективного функціонування комерційних банків, належного рівня їхньої фінансової безпеки неможливе без формування і впровадження дієвої системи виявлення і запобігання фінансовому шахрайству у банківських установах. Аналізуючи сучасну систему безпеки, необхідно дотримуватися простих правил користування програмним забезпеченням та електронними платіжними системами, які застосовуються в усьому світі. Також визначено способи щодо протидії фінансовому шахрайству загалом та операцій із банківськими картками зокрема, що позитивно позначиться на підвищенні рівня фінансової безпеки комерційних банків.

Ключові слова: *банк, банківська діяльність, фінансова безпека, фінансове шахрайство, платіж, фінансові ресурси, банківська картка.*

FINANCIAL FRAUD IN COMMERCIAL BANKS OF UKRAINE. WAYS OF CONTROL IN THE FIELD OF CASHLESS OPERATIONS

The development of non-cash forms of payment, the introduction of bank cards, Internet resources in the field of payments, is a characteristic feature of everyday life. In 2020–2021, due to quarantine measures, Ukrainians increasingly began to choose non-cash payments, payments and online purchases. The active use of the latest information technologies has led to the growth of various manifestations of fraud in the field of public relations, ranging from financial and credit and ending with foreign economic activity and the Internet. Financial fraud, which is a system of relations in the field of money circulation and financial obligations, the purpose of which is to misappropriate the financial resources of banks and/or their customers by deceiving or abusing the trust or position of citizens/employees of banking institutions. The imperfect legal system contributes to the fact that the state continues to actively implement various fraudulent schemes. It has been established that the main type of fraud in the banking sector is payment card fraud. The most common types of fraudulent transactions with bank cards are considered. Based on the analysis of the consequences of cyber-fraud, which occur in the use of payment instruments by banks, it is determined that the most vulnerable place is the client himself, who under the influence of various methods of social engineering becomes the object of fraud. Based on statistical data, the dynamics of the number and structure of crimes related to financial fraud in Ukraine is analyzed and the high level of their latency is emphasized. Emphasis is placed on the important role of the state in overcoming this negative phenomenon. Ensuring the effective functioning of commercial banks, the proper level of their financial security is impossible without the formation and implementation of an effective system for detecting and preventing financial fraud in banking institutions. Analyzing the modern security system, simple rules for using software and electronic payment systems, which are used all over the world, have been introduced. There are also ways to combat financial fraud in general and bank card transactions in particular, which has a positive effect on improving the financial security of a commercial bank.

Keywords: *bank, banking activity, financial security, financial fraud, payment, financial resources, bank card.*

JEL classification: *E42, G20, G21, K42*

Постановка проблеми. Розвиток безготівкових форм розрахунків, впровадження банківських карт, інтернет-ресурсів у сфері платежів є характерною рисою повсякденного життя. У 2020–2021 рр. через карантинні заходи українці все частіше стали вибирати безготівкові платежі, розрахунки та покупки онлайн. Активне використання новітніх інформаційних технологій спричинило зростання різного роду проявів шахрайства у сфері суспільних відносин, починаючи від фінансово-кредитної і завершуючи зовнішньоекономічною діяльністю та мережею Інтернет.

Фінансове шахрайство – це доволі складний, ретельно приховуваний процес ураження фінансової безпеки, що вирізняється широким спектром проявів у процесі функціонування комерційного банку, що супроводжується відчутними збитками для всіх учасників фінансового ринку.

Забезпечення ефективного функціонування комерційних банків (КБ), належного рівня їхньої фінансової безпеки (ФБ) неможливе без формування і впровадження дієвої системи виявлення і запобігання фінансовому шахрайству (ФШ) у банківських установах.

Водночас механізми боротьби з ФШ та їх застосування для забезпечення фінансової безпеки комерційних банків є недостатньо розробленими, а система виявлення, запобігання ФШ у КБ України відсутня, що потребує безвідкладного впровадження у банківську діяльність.

Аналіз останніх досліджень і публікацій. Дослідженнями сутності, способів виявлення та запобігання шахрайству загалом і ФШ зокрема займалися: О.А. Глєбов, О.Ю. Єгорова, А.М. Єрмошенко, М.М. Єрмошенко, Н. Ковтун, Д.Н. Козлов, О.В. Кришевич, В.В. Кулик, В.В. Левін, Ю.В. Михайловська, С. Олбрехт, Л. Пратт, М.С. Савченко, О. Саяпін, Л.В. Сорокіна, І.Б. Ткачук, Г.М. Чернишов, С.С. Чернявський, О.В. Чижов, С.П. Чорнуцький, І.І. Чуницька, П. Шатен, В.І. Ярочків [4]. Найбільш вагомі внески у дослідження фінансового шахрайства здійснили також закордонні автори: С. Альбрехт, Дж. Венц, Т. Вільямс, П. Ліллі, П.А. Лестер, Едвін Х. Сазерленд, Дональд Р. Кressі, Стів Олбрехт, Ричард С. Холлінджер, Дж. Уеллс, Х. Фексеус [6]. Визначенню особливостей, різновидів ФШ у КБ, з'ясуванню його впливу на ФБ КБ, проблематиці механізмів його виявлення і запобігання приділено недостатньо уваги.

Мета статті – дослідити теоретико-концептуальні засади фінансового шахрайства, насамперед з погляду сучасної фінансової науки, та розробити практичні рекомендації з удосконалення механізмів виявлення і запобігання ФШ задля забезпечення ФБКБ.

Виклад основного матеріалу. Концентрація грошей у безготівковій формі, різноманітність фінансових послуг та інструментів із різним рівнем захищеності та ліквідності, клієнтське поле, що розширюється, – усе це робить банківські установи привабливим об'єктом для застосування шахрайських схем та виникнення фінансового шахрайства.

Згідно з Кримінальним кодексом України (ст. 190) під шахрайством розуміється заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою, кримінально каране діяння, за яке в Україні передбачена відповідальність [5].

Фінансове шахрайство – один із найбільш складних видів недобросовісної діяльності, яка набула поширення в банках, що являє собою систему маніпуляцій у сфері банківського грошового обігу у вигляді заволодінням фінансовими ресурсами, набуття прав фінансових вимог та уникнення фінансових зобов'язань [6]. ФШ у КБ свідчить про нездатність останніх забезпечити власну фінансову безпеку на належному рівні. Внаслідок цього уможливлюються фінансові злочини, які неминуче призводять до втрати фінансових ресурсів та, врешті-решт, до позбавлення банківської ліцензії та банкрутства.

Розв'язання завдань із виявлення, протидії та попередження ФШ, які стоять перед кожним КБ, неможливе без розуміння сутності фінансового шахрайства. Слід відзначити, що в науковому середовищі відзначається розрізненість поглядів стосовно поняття «фінансове шахрайство», а також відсутність єдності у підходах із визначення його прояву в КБ [1].

С.С. Мельник у своєму дисертаційному дослідженні «Виявлення та запобігання фінансовому шахрайству у забезпеченні фінансової безпеки комерційних банків» розглядає ФШ через основні сучасні підходи. З позиції науково-теоретичного підходу ФШ відображається як «здійснення протиправних дій у сфері грошового обігу шляхом обману, зловживання довірою чи інших маніпуляцій із метою збагачення» [6].

Кримінальний кодекс України (ККУ) (ст. 222) оперує поняттям «шахрайство з фінансовими ресурсам», яке визначає як «надання завідомо неправдивої інформації органам державної влади, органам влади АР Крим чи органам місцевого самоврядування, банкам або іншим кредиторам із метою одержання субсидій, субвенцій, дотацій, кредитів чи пільг щодо податків» [5].

С.С. Чернявський пропонує розуміти ФШ як комплекс взаємопов'язаних, спільних за криміналістичними ознаками технологій корисливих посягань на фінансові ресурси держави, суб'єктів господарювання та громадян, вчинених шляхом обману і зловживання службовим становищем [9, с. 56].

У межах практично-функціонального підходу ФШ ототожнюється з економічним злочином та визначається, як навмисний обман з метою розкрадання грошових коштів, майна та законних прав. На думку Т. Кізима, фінансове шахрайство – це сукупність економічних відносин, які реалізуються юридичними або фізичними особами (як правило, без насильницьких дій) у процесі формування, розподілу і використання фінансових ресурсів (доходів) шляхом обману або зловживання довірою чи службовим становищем з метою отримання економічної або/та іншої вигоди (особистої, корпоративної чи на користь третіх осіб) [3].

Отже, фінансове шахрайство в комерційних банках – це багатогранне суспільно-економічне явище, що являє собою систему відносин у сфері грошового обігу та фінансових зобов'язань, метою яких є недобросовісне заволодіння фінансовими ресурсами банків і/або їхніх клієнтів шляхом обману або зловживання довірою чи службовим становищем громадян і працівників банківських установ.

Економічна криза додала підстав до активізації банківського шахрайства та появи нових кримінальних ризиків. За статистикою, майже 70% злочинів у банківській сфері здійснюються або винятково співробітниками банку, або за їхньої активної участі. У банківській сфері злочини частіше відбуваються у збанкрутілих банках або у тих, що проходять процедуру санації [4].

Нині найбільш поширеними видами шахрайських операцій є операції з банківськими картками.

1. Соціальна інженерія – введення в оману громадян будь-якими способами для того, щоб вони розголосили власні персональні дані, реквізити платіжних карток, банківські коди та паролі мобільних операторів чи здійснили переказ коштів під психологічним впливом на користь шахраїв. Видами шахрайства шляхом соціальної інженерії є:

– Фішинг – шахрайство за допомогою інтернет-сайтів, створених злочинцями для того, щоб виманювати у користувачів дані їхніх банківських карт. Українською міжбанківською Асоціацією членів платіжних систем (ЕМА) нараховано понад 300 таких сайтів [11].

– Вішинг – шахрайство за допомогою мобільного зв'язку. За опитуванням, 77% українців знають, що нікому не можна повідомляти реквізити картки та коди з банківських SMS. Однак 76%, зіштовхнувшись із мобільним шахрайством, розголошують реквізити своєї картки. Так, середня сума незаконної операції з використанням соцінженерії в першій половині 2020 року становила 3300 гривень. Середня сума незаконної операції в інтернеті становила 195 гривень, як підрахували в ЕМА [11].

Саме тому Національний банк разом з ЄМА запустив Всеукраїнську інформаційну кампанію «Шахрай-Гудбай» з метою протидії платіжному шахрайству шляхом навчання українців основним правилам безпеки безготівкових та онлайн-платежів [11].

2. Шахрайство з банкоматами (додаткове обладнання, злом, підрив) – оснащення банкоматів або POS-терміналів спеціальним пристроєм, який під час взаємодії з карткою зчитує дані. Частіше це відбувається з картками, які оснащені тільки магнітною стрічкою. Фахівці ЕМА радять використовувати картки з чіпом (або безконтактні картки). Але поки що з 39,1 млн активних платіжних карток тільки 6,7 млн оснащені чіпом, за даними НБУ за 9 місяців 2019 року. Решта – це більш вразливі картки на магнітній стрічці [9]. Видами такого шахрайства є:

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

– трапінг – встановлення пасток на шатер банкомату;

– фізичне пошкодження банкоматів.

3. Розкрадання грошей при дистанційному банківському обслуговуванні, вірусні та хакерські атаки тощо.

Окремо слід зазначити, що попит на шахрайські дії з кредитними картками створив ще один вид злочинної діяльності – торгівлю незаконно отриманими особистими даними їх власників, у т.ч. номерами рахунків за кредитними картками, особистою інформацією власників [4].

Найбільша частка шахрайських операцій, які було здійснено за допомогою методів соціальної інженерії (41%), включають у себе здійснення вішингу та фішингу. 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%) [10].

Як повідомляє Департамент комунікацій НБУ, за перші пів року 2020-го зафіксовано 47,5 тисяч випадків шахрайства із платіжними картками на загальну суму 86,4 млн грн (за аналогічним періодом 2019 року було 34,7 тис. таких випадків на 72,6 млн грн). Тобто спостерігається ріст випадків шахрайства, але водночас середній розмір втрат на одну шахрайську операцію зменшився – з 2100 гривень у першій половині 2019 року до 1819 гривень у відповідному періоді 2020 року [8].

А.М. Клочко у своєму дисертаційному дослідженні «Теоретико-прикладні засади протидії злочинам у сфері банківської діяльності в Україні», аналізуючи статистичні дані щодо кількості облікованих кримінальних правопорушень за ст. 200 ККУ «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення» відзначає, що в динаміці за 2014–2018 рр. у структурі злочинів у сфері банківської діяльності спостерігається стрімка тенденція до зростання [4].

Слід сказати, що повної інформації про шахрайство з картковими рахунками на ринку України немає. Враховуючи бездіяльність влади та правоохоронних органів, реальна кількість випадків шахрайства набагато більша. Доступ до цих даних мають тільки банківські установи, але вони їх приховують, дотримуючись вимог Правил міжнародних платіжних систем. Також у вітчизняній фінансовій науці та практиці майже відсутні офіційні статистичні дані стосовно показників фінансового шахрайства, оскільки це поняття фактично відсутнє в українському законодавстві, чого не можна сказати про зарубіжну фінансову науку та практику боротьби із цим видом злочинності [3].

Міжнародні платіжні системи, навпаки, ведуть статистику втрат. Так, Федеральне бюро розслідувань США в офіційних звітах серед економічних злочинів виокремлює інформацію щодо показників фінансового шахрайства [3]. Згідно з даними статистики фінансового шахрайства, у Європі лідерами є Велика Британія і Франція, що несуть набільші збитки від шахрайства з картками порівняно з будь-якими іншими країнами Європи [1]. Так, не дивлячись на інвестиції в передові системи безпеки для захисту клієнтів Великобританії, що запобігли більш ніж £ 1,8 млрд несанкціонованого шахрайства, злочинці успішно вкрали понад 1,2 млрд фунтів стерлінгів через шахрайство й афери в 2019 році. У 2019 році збитки від несанкціонованого фінансового шахрайства в платіжних картках та чеках сягали 824,8 млн фунтів стерлінгів, що на два відсотки більше порівняно з 2018 роком. Найбільш вразливими є операції з платіжними картками, що у структурі фінансових збитків за 2019 р. становлять 48% [12]. Для порівняння, в Україні збитки від шахрайства з картками за 2017–2018 рр. становили в середньому 2,2 млн євро [1].

На основі проведеного аналізу наслідків кібершахрайства, яке відбуваються в сфері використання клієнтами банків платіжних засобів, найбільш вразливим місцем є сам клієнт, який під дією різних методів соціальної інженерії стає об'єктом шахрайства. Для боротьби з цим способом шахрайства українські банки не мають досить дієвих інструментів.

Кіберзлочинці відчувають себе вільно завдяки не тільки низькому рівню фінансової грамотності українців, а й вельми лояльному кримінальному законодавству. ФШ у КБ здійснюється тому, що є впевненість у фінансового шахрая в уникненні відповідальності за

скоєне та можливості зберегти та надалі легалізувати грошові кошти, отримані внаслідок ФШ [4].

В Україні шахрай під час першої судимості несе відповідальність у вигляді лише штрафу. За шахрайство, яке може заподіяти банку збитки на мільйони, передбачено максимальний штраф (ст. 222 КК) у розмірі 180 тис. грн., а мінімальний – 17 тис. грн. [5]. Допоки вартість злочину не буде вищою, аніж його вигода, та не буде встановлена кримінальна відповідальність, існуватимуть злочини у сфері банківської діяльності.

Водночас навіть ліберальний ЄС рекомендує за кібершахрайство призначати перше покарання у вигляді позбавлення волі не менш ніж на один рік. В Іспанії за це можна отримати 12 років, в Польщі – до 25 років, в США – довічні терміни. В Україні у 2016 р. потрапили до в'язниці лише десять шахраїв [7]. Також важливими є система органів, що здійснюють контроль і боротьбу з фінансовим шахрайством. В Україні нині діє лише один такий орган – Департамент кіберполіції Національної поліції України, тобто боротьба із кіберзлочинністю здійснюється лише на правоохоронному рівні, що сьогодні є недостатнім. Для порівняння, у США таких рівнів є три: військовий, правоохоронний та юстиційний, причому кожен із них має особливі повноваження. Тому, відповідно, і боротьба із кіберзлочинністю здійснюється значно ефективніше [4].

Боротьба КБ із ФШ у забезпеченні ФБКБ має спрямовуватися на: підвищення обізнаності громадян та персоналу КБ про ознаки ФШ та способи його розпізнавання, виявлення, розслідування, запобігання, протидії, мінімізації негативних наслідків [4]. Оскільки шахраїв можна поділити на тих, які націлені на приватних клієнтів банку і на саму фінансову установу, щоб уникнути ризику втрати грошей внаслідок кібератаки, необхідно дотримуватися простих правил користування програмним забезпеченням та електронними платіжними системами (таблиця 1).

Щодо забезпечення належного рівня фінансової безпеки банківського платіжного середовища в банках України вже запроваджено:

– Відкритий банкінг – систему, за допомогою якої банки відкривають інтерфейси програмування прикладних програм (API), дозволяючи третім сторонам отримувати доступ до фінансової інформації, необхідної для розроблення нових додатків та послуг та надаючи власникам рахунків більші можливості фінансової прозорості [1].

– Найпоширеніший спосіб аутентифікації оплати за допомогою онлайн-картки покладається на 3D Secure – стандарт аутентифікації, який підтримує переважна більшість європейських карток.

– Функціонування міжгалузевої онлайн-системи обміну інформацією між банками, процесинговими центрами України і близького зарубіжжя, а також правоохоронними органами про платіжне (з платіжними інструментами і сервісами), кредитне і кібершахрайство,

Таблиця 1

Способи захисту інформації та протидії банківському шахрайству

Для приватних клієнтів банку:
1) ніколи нікому не розголошувати свої паролі, CVV чи PINкоди; 2) не переходити за підозрілими посиланнями, вони здебільшого розроблені для завантаження зловмисного програмного забезпечення на пристрій; 3) не відкривати та не зберігати незнайомі файли на своєму пристрої; 4) бути обережними під час використання загальнодоступних мереж Wi-Fi, оскільки вони можуть бути небезпечними та ненадійними; 5) якщо сайт здається підозрілим або незнайомим, не потрібно вводити дані своєї платіжної картки та не робити покупки; 6) завантажувати додатки Інтернет-банкінгу з Google Play Market або iOS App Store; 7) використовувати для платежів лише веб-сайти, які починаються з HTTPS: //, вони мають систему захисту 3D Secure; 8) якщо платіжна картка прив'язана до номера телефону, який знають знайомі і який опублікований на ваших сторінках у соцмережах, – зверніться до мобільного оператора з паспортом і попросіть ідентифікувати вас тільки за наявності цього документу. 9) зачекайте хвилинку, перш ніж розлучитися з грошима або інформацією, що тримає вас у безпеці. Запитайте себе: Чи може це бути підробкою? Якщо вважаєте, що ви потрапили на шахрайство, негайно зв'яжіться зі своїм банком.
Для банківської установи:
1) інвестувати в регулярні навчання з інформованості про кібербезпеку для працівників, щоб навчити їх не натискати на посилання або відкривати вкладення, отримані з підозрілих джерел; 2) регулярно проводити тестові фішинг-атаки, щоб переконатися, що працівники знають, як розрізняти фішинг-листи; 3) при використанні хмарних сервісів електронної пошти необхідно переконатися, що є встановлено спеціальний захист від спам-атак електронної пошти; 4) переконатися, що всі рівні корпоративного програмного забезпечення надійно захищені – від основних центрів обробки даних до спеціалізованих систем (наприклад, банкоматів); оновлювати застарілі версії програмного забезпечення; 5) для АТМ і POS використовувати рішення, розроблені спеціально для цих систем, які захищають пристрої навіть зі слабким або застарілим обладнанням; 6) здійснювати моніторинг операцій з використанням електронних платіжних засобів (та/або їх реквізитів) в режимі 24/7; 7) у внутрішньобанківських правилах та договорі з клієнтом банкам необхідно враховувати можливість врегулювання нестандартних ситуацій у процесі здійснення операцій із використанням платіжних карток та розглядати звернення/скарги клієнта відповідно до умов договору, а не відправляти в поліцію, яка фактично нічого не робить; 8) проводити термінове розслідування за допомогою служби безпеки між банками, що здійснили операцію яку провели шахраї, блокувати рахунки і не давати злочинцям можливості зняти гроші 9) здійснювати повну ідентифікацію, верифікацію клієнта (представника клієнта), вивчення клієнта та уточнення інформації про клієнта, забезпечувати у своїй діяльності управління ризиками.

Джерело: [1]

інциденти інформаційної безпеки – «Exchange-online», що розроблено ЕМА і не має аналогів у світі [4].

Серед шляхів протидії фінансовому шахрайству у КБ варто виділити таке:

1. Підвищення обізнаності громадян України про ефективні способи захисту власної інформації та правила безпечного використання платіжних карток, електронних платежів і банкоматів.

2. Покращення якості обслуговування власників банківських карт і можливість запобігання і виявлення нових видів шахрайства за допомогою впровадження спеціальної системи надання авторизації (блокування операцій та подвійна (потрійна) ідентифікація клієнта); технічне забезпечення банкоматів, включаючи антискімінгові пристрої, установку антивірусних програм і вдосконалення структури карт, в тому числі випуск «чіпованих» карт за новим стандартом EMV (технологія ЧІП та ПІН), а також створення додатків безпеки, зокрема додаток 3D Secure для операцій онлайн.;

3. Випуск платіжних карт без реквізитів (відсутні номер карти, термін дії та CVV), що вже запровадив Альфабанк Україна та Monobank. Пластик матиме лише ім'я та прізвище власника карти. Ідентифікаційна інформація для проведення платежів буде перенесена в мобільний додаток Інтернет-банкінгу відповідного банку; використання нової технології Visa Token Service, або просто VTS що розпочав застосовувати у своїй роботі Ощадбанк. VTS дозволить встановити абсолютно новий рівень безпеки і захисту персональних даних клієнтів банку, що здійснює онлайнові платежі. Замість реквізитів платіжної картки буде використовуватися унікальний токен, цифровий ідентифікатор користувача. Всі оплати будуть здійснюватися за допомогою цифрової копії карти.

4. 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 [10];

5. Жорстке обмеження прав доступу працівників банків, до бази даних клієнтів для зменшення шахрайств з боку працівників;

6. Розроблення стратегії боротьби з ФШ у КБ; оперативне розслідування повідомлень про фактичні й імовірні випадки ФШ у КБ, інформації про злочини з платіжними картками, електронними платежами в банкоматах; вдосконалення взаємодії між банками, патрульною поліцією, кіберполіцією і слідством під час розслідування та протидії злочинам із платіжними картками, електронними платежами і з банкоматами;

7. Удосконалення кримінального законодавства України у сфері неправомірного використання засобів платежу і поширених видів карткових і платіжних злочинів та приведення його у відповідність до світових стандартів. Запровадити досвід США щодо правового регулювання боротьби із кіберзлочинністю;

8. Отримання послуг страхування банківської карти. При цьому необхідне формування резервів або за рахунок банку, або у вигляді страховки, які дозволять компенсувати втрачені кошти клієнтам банків [2].

Висновки. Фінансове шахрайство в комерційних банках – це багатогранне суспільно-економічне явище, що являє собою систему відносин у сфері грошового обігу та фінансових зобов'язань, метою яких є недобросовісне заволодіння фінансовими ресурсами банків і/або їх клієнтів шляхом обману або зловживання довірою чи службовим становищем громадян і працівників банківських установ.

З'ясовано, що основним видом шахрайства в банківській сфері є шахрайство з платіжними картками. Розглянуто найбільш поширені види шахрайських операцій з банківськими картками. На основі проведеного аналізу наслідків кібершахрайства, які відбуваються в сфері використання клієнтами банків платіжних засобів, визначено що найбільш вразливим місцем є сам клієнт, який під дією різних методів соціальної інженерії стає об'єктом шахрайства. На основі статистичних даних проаналізовано динаміку кількості та структури злочинів, пов'язаних із фінансовим шахрайством в Україні, та наголошено на високому рівні їх латентності. Акцентовано на важливій ролі держави у подоланні цього негативного явища.

Застосування в банківському платіжному середовищі сучасних цифрових технологій потребує від комерційних банків особливу увагу звертати на фінансову безпеку задля збереження як клієнтів, так і фінансової стабільності самої установи. Аналізуючи систему безпеки за кордоном та стан сучасної системи боротьби з ФШ, запроваджено дотримуватися простих правил користування програмним забезпеченням та електронними платіжними системами, які застосовуються в усьому світі. Також для забезпечення фінансової безпеки банківського платіжного середовища банківським установам визначено способи щодо протидії фінансовому шахрайству та операціям із банківськими картками.

Список використаних джерел:

1. Дубина М.В., Садчикова І.В., Середюк І.О. Концептуальні підходи до підвищення рівня безпечності банківського платіжного середовища України. URL: https://www.business-inform.net/export_pdf/business-inform-2020-3_0-pages-349_359.pdf

2. Кривошапова С.В., Литвин Е.А. Оценка и способы борьбы с мошенничеством с банковскими картами в России. URL: https://www.elibrary.ru/download/elibrary_23213322_81349007.pdf

3. Кізима Т. Фінансове шахрайство: теоретична концептуалізація та економічне підґрунтя. URL: http://sf.wunu.edu.ua/index.php/sf/article/view/1230

4. Клочко А.М. Теоретико-прикладні засади протидії злочинам у сфері банківської діяльності в Україні : дис. доктора юридичних наук : 12.00.08. Київ, 2020. 563 с.

5. Кримінальний кодекс України (поточна редакція). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

6. Мельник С.С. Сутність фінансового шахрайства в комерційному банку. *Науковий вісник Ужгородського національного університету*. 2016. № 6 (ч. 2). С. 91–95.

7. Олійничук.О. Банківські картки як об'єкт шахрайства: стан і протидія явищу. URL: http://dspace.tneu.edu.ua/handle/316497/24516

8. Національний банк України. URL: https://bank.gov.ua/

9. Чернявський С.С. Фінансове шахрайство: методологічні засади розслідування : [монографія]. Київ : Хай-Тек Прес, 2010. 624 с.

10. Яровенко Г.М. Аналіз наслідків кібершахрайств в банківській системі України. URL: http://economyandsociety.in.ua/journals/18_ukr/116.pdf
11. Українська міжбанківська асоціація членів платіжних систем EMA. URL: https://www.ema.com.ua/
12. Fraud – The Facts 2020. URL: https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2020

References:

1. Dubyna M.V., Sadchykova I.V., Seredyuk I.O. Kontseptual'ni pidkhody do pidvyshchennya rivnya bezpechnosti bankivs'koho platizhnoho seredovyshcha Ukrayiny. Available at: https://www.business-inform.net/export_pdf/business-inform-2020-3_0-pages-349_359.pdf
2. Kryvoshapova S.V., Lytvyn E.A. Otsenka i sposoby borot'by shakhraystva z bankivs'kymy kartkamy v Rossyy. Available at: https://www.elibrary.ru/download/elibrary_23213322_81349007.pdf
3. Kizyma T. Finansove shakhraystvo: teoretychna kontseptualizatsiya ta ekonomichne pidgruntya. Available at: http://sf.wunu.edu.ua/index.php/sf/article/view/1230
4. Klochko A.M. (2020). Teoretyko-prykladni zasady protydiyi zlochynam u sferi bankivs'koyi diyal'nosti v Ukrayini: dys. doktora yurydychnykh nauk: 12.00.08. Kyiv, 563 p.
5. Kryminal'nyy kodeks Ukrayiny (potochna redaktsiya). Available at: https://zakon.rada.gov.ua/laws/show/2341-14#Text6
6. Mel'nyk S.S. (2016). Sutnist' finansovoho shakhraystva v komertsiynomu banku. *Naukovyy visnyk Uzhhorods'koho natsional'noho universytetu*, vol. 6 (ch. 2), pp. 91–95.
7. Oliynychuk O. Bankivs'ki kartky yak ob"yekt shakhraystva: stan i protydiya yavyshchu. Available at: http://dspace.tneu.edu.ua/handle/316497/24516
8. Natsional'nyy bank Ukrayiny. Available at: https://bank.gov.ua/
9. Chernyavs'ky S.S. (2010) Finansove shakhraystvo: metodolohichni zasady rozsliduvannya: [monohrafiya]. Kyiv: Khay-Tek Pres, 624 p.
10. Yarovenko H.M. Analiz naslidkiv kibershakhraystv v bankivs'kiy systemi Ukrayiny. Available at: http://economyandsociety.in.ua/journals/18_ukr/116.pdf
11. Ukrayins'ka mizhbankivs'ka asotsiatsiya chleniv platizhnykh system EMA. Available at: https://www.ema.com.ua/
12. Fraud – The Facts 2020. Available at: https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2020