

**Ключові слова:** соціальний аудит, контроль, корпоративна соціальна відповідальність, аудиторський звіт, соціально-економічна система.

**Мазуренок О.Р., Плекан У.М. СОЦИАЛЬНЫЙ АУДИТ КАК ИНСТРУМЕНТ ОЦЕНКИ КОРПОРАТИВНОЙ СОЦИАЛЬНОЙ ОТВЕТСТВЕННОСТИ**

**Цель.** Анализ сущности и технологии проведения социального аудита на корпоративном уровне.

**Методика исследования.** Теоретическую основу исследования составили основные категории и концептуальные положения социального аудита и организации его проведения на корпоративном уровне. В процессе исследования использовался диалектический подход при определении причинно-следственных связей в процессе социального аудита и влияния реализованных социальных инициатив на результаты основной деятельности компаний. Применяются методы анализа, выявлены критерии организации корпоративной социальной ответственности и сгруппированы показатели социального аудита, отражающие состояние социальной сферы компаний. Большое значение имели методы системно-структурного анализа и синтеза – при оценке задач и функций социального аудита и определении классификации социального аудита в соответствии с основными признаками.

**Результаты исследования.** Исследованы сущность и особенности социального аудита, его значимость и влияние на развитие корпораций и общества в целом. Доказана важность социального аудита в финансово-экономической системе в качестве базиса экономических интересов компаний и определена необходимость его внедрения с целью утверждения социально ответственной деятельности бизнес-структур. Описаны процессы развития социального аудита в мире и особенности его становления в Украине. Исследованы задачи и функции социального аудита, приведена его классификация в соответствии с основными признаками, определены базовые характеристики социального аудита. На основании проанализированных литературных источников описана технология проведения социального аудита компаний.

**Научная новизна результатов исследования.** Предложены базовые критерии организации корпоративной социальной ответственности и сгруппированы показатели социального аудита, что, в отличие от существующих, обеспечивают более полное отражение состояния социальной сферы компаний.

**Практическая значимость результатов исследования.** Результаты научных разработок и практические рекомендации, приведенные в статье, могут быть использованы отечественными компаниями при разработке эффективной технологии социального аудита для развития социально ответственной сферы деятельности.

**Ключевые слова:** социальный аудит, контроль, корпоративная социальная ответственность, аудиторский отчет, социально-экономическая система.

**Mazurenok O.R., Plekan U.M. SOCIAL AUDIT AS TOOL FOR ASSESSING CORPORATE SOCIAL RESPONSIBILITY**

**Purpose.** The aim of the article is to analyze the essence of social audit and realization of technologies of social audit of companies.

**Methodology of research.** The foundation of this article is comprised of basic categories and concepts of social audit and steps in conducting social audit of companies. The dialectic approach is used in research to determine the cause-effect relationships, how they affect realization of social audit and what impact those social initiatives have on the main results of primary activity of companies in question.

The basic criteria of organization of social activity of companies are determined in research due to the use of analysis methods and the indicators of social audit that reflect the state of the social sphere of companies are suggested.

A big role in this was attributed to the methods of systematic structured analysis and synthesis to evaluate the tasks and functions of social audit, and a role in determining of its classification according to main characteristics.

**Findings.** The article gives an in-depth explanation of essence and characteristics of social audit. The importance of social audit and its impact on the development of corporations and society at large are analyzed. The importance of social audit in the financial and economic systems as the main basis of the company economic interests is developed and the necessity of its introduction with the aim of establishing socially responsible economic activity of businesses is determined.

A research of the development of social audit at the international level is conducted. The processes of social audit development and peculiarities of its formation in Ukraine are investigated. Its goal and functions are proved. The classification of social audit according to its main characteristics is given. The basic criteria of organization of social activity of companies are offered. Realization of technologies of social audit of companies is suggested on the basis of analyzed literary sources.

**Originality.** The basic criteria of organization of social activity of companies are offered and the indicators of social audit that unlike the existing ones provide a better reflection of the state of the social sphere of companies are suggested.

**Practical value.** Practical importance of the obtained results is in the possibility of using both scientific development findings and practical recommendations from the article for various domestic companies to elaborating efficient technologies of social audit for the development of socially responsible sphere of activity.

**Key words:** social audit, control, corporate social responsibility, auditor's report, social and economic system.



**Кушнерьов О.С. ТЕНДЕНЦІЇ ШАХРАЙСЬКИХ ОПЕРАЦІЙ НА БАНКІВСЬКОМУ РИНКУ ТА МОЖЛИВОСТІ ПРОТИДІЇ**

**Мета.** Визначення тенденцій шахрайської діяльності та окресленні можливостей протидії шахрайству на банківському ринку України та інших країн світу.

**Методика дослідження.** Основою методики даного дослідження є порівняльний, динамічний, структурний аналіз. В частині дослідження видів шахрайських операцій застосовується класифікація, індукція та дедукція. Широко застосовується графічний метод. Дані методи використано при визначенні обсягів втрат шахрайських операцій; при визначенні структури фінансових втрат в розрізі різновидів шахрайських операцій; при визначенні тенденцій у банківському шахрайстві.

**Результати дослідження.** На основі інформації щодо об'ємів шахрайських операцій проаналізовано їх структуру, а також визначено попередні прогностичні характеристики щодо розвитку ситуації щодо шахрайських операцій на українському та іноземних банківських ринках. Визначено, що Україна знаходиться серед країн, де ризик такого роду шахрайства є помірним. Проте, особливості розвитку і постійного вдосконалення методів, використовуваних зловмисниками, ставить задачу розробки гнучких та ефективних методів виявлення потенційних загроз шахрайства та запобігання їх реалізації. Також проаналізовано обсяги та структуру шахрайських операцій в розрізі глобального ринку. Детально проаналізовано структуру банківського шахрайства по типах застосовуваних технологій, розглянуто динаміку обсягу деяких видів шахрайських операцій та визначено основні заходи протидії банківському шахрайству. Відзначено, що найбільш ефективним заходом щодо протидії шахрайським операціям з боку клієнтів банків є максимальна поінформованість користувачів щодо необхідних дій в разі шахрайських атак або з метою їх запобігання.

**Наукова новизна результатів дослідження.** Визначено основні характерні особливості банківських шахрайських операцій та їх сегментації за «цільовою аудиторією» потенційних жертв.

**Практична значущість результатів дослідження.** Результати представленого дослідження дозволяють на основі запропонованого структурно-динамічного аналізу виявляти зміни, структуру та тенденції в сфері банківського шахрайства, а також у відповідності до визначених тенденцій будувати політику протидії шахрайству.

**Ключові слова:** транзакції, шахрайство, шахрайські операції, технології, тенденції, структура.

#### **Кушнерев А.С. ТЕНДЕНЦИИ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ НА БАНКОВСКОМ РЫНКЕ И ВОЗМОЖНОСТИ ПРОТИВОДЕЙСТВИЯ**

**Цель.** Определение тенденций мошеннической деятельности в области банковских транзакций и поиск возможности противодействия мошенничеству на банковском рынке Украины и других стран мира.

**Методика исследования.** Основой методики данного исследования является сравнительный, динамический, структурный анализ. В части исследования видов мошеннических операций применяется классификация, индукция и дедукция. Широко применяется графический метод.

**Результаты исследования.** На основе информации по объемам мошеннических операций проанализирована их структура, а также определены предварительные прогностические характеристики по развитию ситуации по мошенническим операциям на украинском и иностранных банковских рынках. Определено, что Украина находится в числе стран, где риск такого рода мошенничества является умеренным. Однако, особенности развития и способность мошеннических технологий к постоянному совершенствованию ставит задачу разработки гибких и эффективных методов выявления потенциальных угроз мошенничества и предотвращения их реализации. Также проанализированы объемы и структура мошеннических операций в разрезе глобального рынка. Подробно проанализирована структура банковского мошенничества по типам применяемых технологий, рассмотрена динамика объема некоторых видов мошеннических операций и определены основные меры противодействия банковскому мошенничеству. Отмечено, что наиболее эффективной мерой по противодействию мошенническим операциям со стороны клиентов банков является максимальная осведомленность пользователей о необходимых действиях в случае мошеннических атак или для их предотвращения.

**Научная новизна результатов исследования** заключается в определении основных отличительных особенностей банковских мошеннических операций и их сегментации по «целевой аудитории» потенциальных жертв.

**Практическая значимость результатов исследования.** Результаты представленного исследования позволяют на основе предложенного структурно-динамического анализа выявлять изменения, структуру и тенденции в сфере банковского мошенничества, а также в соответствии с определенным характером тенденций строить политику противодействия мошенничеству.

**Ключевые слова:** транзакции, мошенничество, мошеннические операции, технологии, особенности, структура, тенденции.

#### **Kushnerov O.S. TRENDS OF FRAUDULENT TRANSACTIONS IN THE BANKING MARKET AND OPPORTUNITIES FOR COUNTERACTION**

**Purpose.** The main of the article is determining the trends of fraudulent activity and outlining the possibilities of counteracting fraud in the banking market of Ukraine and other countries of the world.

**Methodology of research.** The basis of the methodology of this study is comparative, dynamic, structural analysis. Classification, induction and deduction are used in the study of types of fraudulent operations. The graphic method is widely used. These methods are used in determining the amount of losses of fraudulent operations; in determining the structure of financial losses in the context of types of fraudulent transactions; when determining trends in banking fraud.

**Findings.** The structure of fraudulent transactions is analyzed on the basis of information according their volumes, as well as the preliminary forecast characteristics for the development of the situation regarding fraudulent transactions in the Ukrainian and foreign banking markets. It has been determined that Ukraine is among the countries where the risk of such fraud is moderate. However, the peculiarities of the development and continuous improvement of the methods used by the attackers poses the task of developing flexible and effective methods for identifying potential fraud threats and preventing their implementation.

Also, the volume and structure of fraudulent transactions in the context of the global market are analyzed. The structure of banking fraud by types of technologies used is analyzed in detail, the dynamics of the volume of certain types of fraud operations is considered, and the main measures to counter banking fraud are determined. It is noted that the most effective measure to counter fraudulent transactions by bank customers is to maximize the awareness of users about the necessary actions in case of fraudulent attacks or in order to prevent them.

**Originality.** The main features of banking fraud operations and their segmentation by “target audience” of potential victims are identified.

**Practical value.** The results of the presented study allow to identify changes, structure and tendencies in the field of banking fraud based on the proposed structural and dynamic analysis, as well as to create a policy of counteracting fraud in accordance with the identified tendencies.

**Key words:** transactions, fraud, fraudulent transactions, technologies, trends, structure.





# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕКОНОМІЧНА БЕЗПЕКА

УДК 336.7

JEL Classification: G21

Кушнерьов О.С.,  
аспірант\* кафедри економічної кібернетики,  
Навчально-науковий інститут  
бізнес-технологій "УАБС" (м. Суми)

## ТЕНДЕНЦІЇ ШАХРАЙСЬКИХ ОПЕРАЦІЙ НА БАНКІВСЬКОМУ РИНКУ ТА МОЖЛИВОСТІ ПРОТИДІЇ\*

Kushnerov O.S.,  
postgraduate student at the department  
of economic cybernetics,  
Education and Research Institute for  
Business Technologies «UAB» (Sumy)

## TRENDS OF FRAUDULENT TRANSACTIONS IN THE BANKING MARKET AND OPPORTUNITIES FOR COUNTERACTION

**Постановка проблеми.** Банківські транзакції стають все більш чисельними. З розвитком банківських технологій удосконалюються транзакційні інструменти. Fin Tech (фінансові технології) обумовлюють значні переваги безготівкових розрахунків над готівковими. Практично всі аспекти грошового обігу сьогодні пристосовані до безготівкових операцій [19]. Це є фактором здешевлення транзакційних витрат, а також фактором привабливості безготівкового обігу для клієнтів [9]. Але завжди існує можливість «паразитарного», злочинного використання технологічних можливостей цифрового банкінгу. Тому дослідження тенденцій шахрайства в сфері банківських операцій є завжди актуальним.

Світовий банківський ринок перейшов у «цифрову» площину і безготівкові операції становлять переважну більшість серед транзакцій [11]. Відстеження тенденцій, прогноз подальшої динаміки шахрайських операцій по усіх їх типах важливий для виявлення найбільш небезпечних сегментів в загальному обсязі шахрайських транзакцій. Відтак важливим стає визначення тенденцій розвитку даного явища на банківському ринку з метою розробки превентивних заходів щодо протидії шахрайству у банківській сфері.

Існує безліч видів шахрайства в банківській сфері і серед них можна виділити чотири основні групи. Першу групу утворюють схеми розкрадання грошових коштів шляхом їх отримання за підробленими банківськими документами і цінними паперами, наприклад: розрахунковими чеками, векселями, депозитними сертифікатами і т.д. Другу групу складають розкрадання грошових коштів вкладників і інвесторів, отриманих під обіцянку виплати високих відсотків або виконання інших зобов'язань (за принципом фінансових пірамід чи інших «пірамід»). Суть такого шахрайства полягає в тому, що зобов'язання перед новими вкладниками виконуються на першому етапі за рахунок надходження коштів нових інвесторів і їх обману. До наступної групи відноситься кредитне шахрайство, яке представляє собою розкрадання грошових коштів шляхом отримання різних кредитів з наданням підробленої документації. В цьому випадку обман полягає в: поданні завідомо неправдивих відомостей; поданні завідомо недостовірних відомостей; поданні завідомо неправдивих і недостовірних відомостей. Даний вид шахрайства в банківській сфері є найпоширенішим і зловмисники використовують його частіше за інших. Потенційний позичальник надає банку або іншому

\* Науковий керівник – Яровенко Г.М. – канд. екон. наук, доц.

\* 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»

кредитору завідомо неправдиві і (або) недостовірні відомості у вигляді документів, що підтверджують його уявну платоспроможність, які в подальшому повинні бути ретельно перевірені кредитною організацією. Четверту групу утворює шахрайство з використанням банківських карт (чужих або підроблених кредитних, розрахункових чи інших платіжних). Даний вид шахрайства є порівняно новим і активно розвивається.

Види шахрайства в такій сфері дуже різноманітні. Більш того, шахраї стали активно використовувати досягнення технічного прогресу, в зв'язку з чим з'являються нові витончені види шахрайських дій в зазначеній галузі [10].

Надзвичайно важливою є проблема наслідків банківського шахрайства для банків та їх клієнтів. Зокрема, найбільшу небезпеку представляє те, що, по суті, у переважній кількості випадків відшкодування втрачених коштів є проблематичним, або й неможливим [8]. Так, якщо, наприклад, у випадку «банкоматного» шахрайства зловмисник, що монтує шахрайські пристрої на банкомат, може бути відстежений за допомогою відеокамери і затриманий під час зняття такого пристрою (або ж, як оптимальний варіант, сам пристрій може бути оперативним знятий), то у випадку застосування методів соціальної інженерії повернення коштів ускладнюється тим, що жертва практично сама віддає свої кошти шахраям. Так, при традиційній схемі СМС-фішингу, коли клієнт вносить «завдаток» за нібито отриманий ним несподівано виграш, або у випадку самостійного переказу коштів клієнтом за неіснуючий або завідомо менш вартісний товар, повернути кошти є неможливим з огляду на те, що така схема є короткотерміною, і зловмисники зникають швидше, ніж стає зрозумілим, що це саме шахрайська схема [20]. Або, якщо вести мову про іншу подібну шахрайську схему, що донедавна використовувалася надзвичайно масово, а саме, про схему з умовною назвою «вашу карту буде заблоковано», то жертва, що зателефонувала на вказаний номер підставної «гарячої лінії», і сама передала усі дані своєї карти зловмиснику, а також повідомила захисний код, при втраті контролю над своїм картрахунком (сам факт втрати жертва, як правило, виявляє після втрати коштів) ні банк, ні жертва не можуть повернути втрачене перш, ніж буде знайдено зловмисників. Отже, оскільки знайти зловмисників у таких випадках практично неможливо (і не в останню чергу через короткотривалий характер існування організаційної структури схеми, що включає телефонний номер, місце розташування виконавця та самого виконавця), кошти будуть втрачені безповоротно.

В цілому, що стосується українського ринку, то на ньому найбільш розповсюдженими є саме методи соціальної інженерії. Ці методи спираються на здійснення психологічного впливу на жертву з метою підштовхування останньої до здійснення необхідних для зловмисників дій. За даними ЄМА (Української міжбанківської асоціації членів платіжних систем) на кінець 2018 р. близько 70% – це шахрайські операції, пов'язані з соціальною інженерією та здійснені за допомогою мережі Інтернет [18]. Банкоматне шахрайство складає приблизно четверту частину від усієї кількості шахрайських операцій та має тенденцію до зниження своєї частки у зв'язку з удосконаленням банківських технологій захисту банкоматів. Протягом 2017–2018 рр. значно зменшилася й до цього незначна частка шахрайських операцій через POS-термінали та дещо зросла частка випадків шахрайства при дистанційному банківському обслуговуванні.

Не варто виключати і можливостей співучасті в тій чи іншій шахрайській схемі з боку працівників банків. Це – ще один з напрямків «роботи» шахрайських схем. Працівники банку можуть не лише надавати зловмисникам дані клієнтів за грошову винагороду, але й бути активними учасниками схем, а подекуди – й організаторами.

Величезним сегментом шахрайства є технологічний сегмент. Тобто, за допомогою застосування технологічних рішень зловмисники отримують дані клієнтів банків, або й безпосередній доступ до банківських рахунків жертв (цю «задачу» виконують, як правило, фішингові технології) [5].

З 2016 р. VISA і MasterCard ввели принцип нульової відповідальності в Україні та на глобальному рівні. Це означає, що якщо власник карт цих платіжних систем став жертвою шахраїв і зміг це довести, то банки повинні компенсувати йому кошти. Це ставить проблему запобігання шахрайським операціям з боку банків. Отже, даний аспект є позитивним для клієнтів банків не лише з огляду на можливість компенсації навіть безнадійно втрачених коштів, а й, що найбільш важливо, з огляду на те, що інвестиції банків у технології захисту від шахрайства є вже об'єктивно обумовленими інтересами самих банків. Отже, постійна робота з боку банків над удосконаленням систем безпеки транзакцій та систем захисту даних своїх клієнтів буде тривати й надалі.

**Аналіз останніх досліджень і публікацій.** Тема протидії шахрайству в сфері банківських операцій знаходиться в полі постійної уваги науковців. Щодо платіжного шахрайства у безготівкових розрахунках, цікавими є дослідження таких авторів, як: О. І. Барановський, С. В. Поперешняк, С. С. Мельник, В. П. Сухонос, К. С. Chakrabarty, Antonio D'Albore та інших. Автори розглядають різноманітні типи шахрайських операцій та пропонують як емпіричні моделі процесів у шахрайських транзакціях, так і математичні моделі, які допомагають діагностувати можливі шахрайські операції. Це надзвичайно важливо в запобіганні проведення шахрайських транзакцій.

Темі запобігання шахрайству в банківській сфері, а саме оцінюванню ризиків шахрайських операцій, присвячені роботи Н. В. Кузнєцової, Т. В. Романенко та ін. В дослідженнях Н. В. Кузнєцової

висвітлюються питання скорингу, як аналітичного методу визначення тенденцій шахрайства та прогнозування шахрайських операцій за кредитними картками за допомогою математичного моделювання. Автор використовує модель багат шарового перцептронну як модель виявлення шахрайських операцій.

Значний вклад у розробку питань, пов'язаних з ідентифікацією шахрайських операцій у банках, зроблено Г. М. Яровенко. Зокрема, автор вказує на можливість виявлення ознак шахрайства клієнтів та працівників банків за допомогою інформаційних моделей [7], а також за допомогою економетричних моделей різного типу, пропонуючи при цьому логістичні моделі, а також моделі, що базуються на нейронній мережі, як інструменти аналізу з метою запобігання здійсненню шахрайських операцій.

Одночасно, у зв'язку з динамічним характером банківського шахрайства, а також відмінностями шахрайських технологій у залежності від сфери їх застосування актуальним залишається питання визначення тенденцій у динаміці та структурі шахрайських операцій та їх прогнозування для подальшого запобігання втратам від банківського шахрайства.

**Постановка завдання.** Мета дослідження полягає у визначенні тенденцій шахрайської діяльності та окресленні можливостей протидії шахрайству на банківському ринку України та інших країн світу.

**Виклад основного матеріалу дослідження.** Шахрайство у банківській сфері є достатньо різноманітним. Перш за все, за суб'єктом вчинення шахрайських дій воно може поділятися, як: шахрайство з боку працівників банку; шахрайство з боку клієнтів банку; шахрайство з боку третіх осіб по відношенню до працівників чи клієнтів банку [13]. Окрім того, за об'єктом вчинення шахрайських дій воно може бути розподілене, як: шахрайство щодо банків та банківської інфраструктури; шахрайство щодо клієнтів. За сферами скоєння шахрайських дій його можна розділити на чотири групи (табл. 1).

Таблиця 1

## Типологія шахрайських операцій у банківській сфері

№ з/п	Тип шахрайства	Види шахрайських операцій
1	Шахрайство з банківськими картками	<ul style="list-style-type: none"> <li>– крадіжка персональної інформації;</li> <li>– крадіжка або навмисна втрата банківської карти;</li> <li>– шахрайство через Інтернет або телефон;</li> <li>– виготовлення дубліката картки;</li> <li>– подвійна транзакція;</li> <li>– крадіжка даних по карті або ПІН-коду.</li> </ul>
2	Депозитне шахрайство	<ul style="list-style-type: none"> <li>– заниження офіційної суми депозиту в банківських документах;</li> <li>– списання грошових коштів з депозитного рахунку клієнта.</li> </ul>
3	Кредитне шахрайство	<ul style="list-style-type: none"> <li>– оформлення кредиту за чужими паспортними даними;</li> <li>– незаконне перерахування грошових коштів на чужі рахунки.</li> </ul>
4	Шахрайство в розрахунково-касовому обслуговуванні	<ul style="list-style-type: none"> <li>– фальшиві банкноти;</li> <li>– додаткові відрахування з банківського рахунку клієнта;</li> <li>– зчитування карти жертви.</li> </ul>

Джерело: складено автором на основі [1]

Отже, за походженням шахрайські операції в банківській сфері можуть бути зовнішніми (здійснюються клієнтами банку або третіми особами) і внутрішніми (здійснюються персоналом банку).

В даному дослідженні розглядаються шахрайські операції транзакційного типу, об'єктом яких є банківські платіжні картки.

Щодо банківського шахрайства (як, втім, і будь-якого іншого) варто відзначити найбільш характерну особливість – гнучкість. Дійсно, з появою нових банківських технологій виникають і нові шахрайські технології, спрямовані на використання усіх їх можливих прогалів.

Перш за все, необхідно уточнити визначення терміну «шахрайство» стосовно банківських операцій.

С. Чакрабарті стверджує, що у загальному аспекті шахрайство визначається як будь-яка дія, за допомогою якої людина має намір отримати блага в протизаконний спосіб [1, с. 2]. Іншими словами, за визначенням А. Д'Альборе, шахрайство – це дії або бездіяльність, направлені на отримання неправомірної вигоди певною особою за рахунок втрат іншої особи [2]. С. С. Чернявський [6, с. 56] фінансове шахрайство визначає як кримінальне явище, розуміючи його як «комплекс взаємопов'язаних і спільних за криміналістичними ознаками технологій корисливих посягань на фінансові ресурси держави, суб'єктів господарювання та громадян, учинених шляхом обману й зловживання службовим становищем». Дане визначення виявляє сутність шахрайських транзакцій достатньо точно і повно.

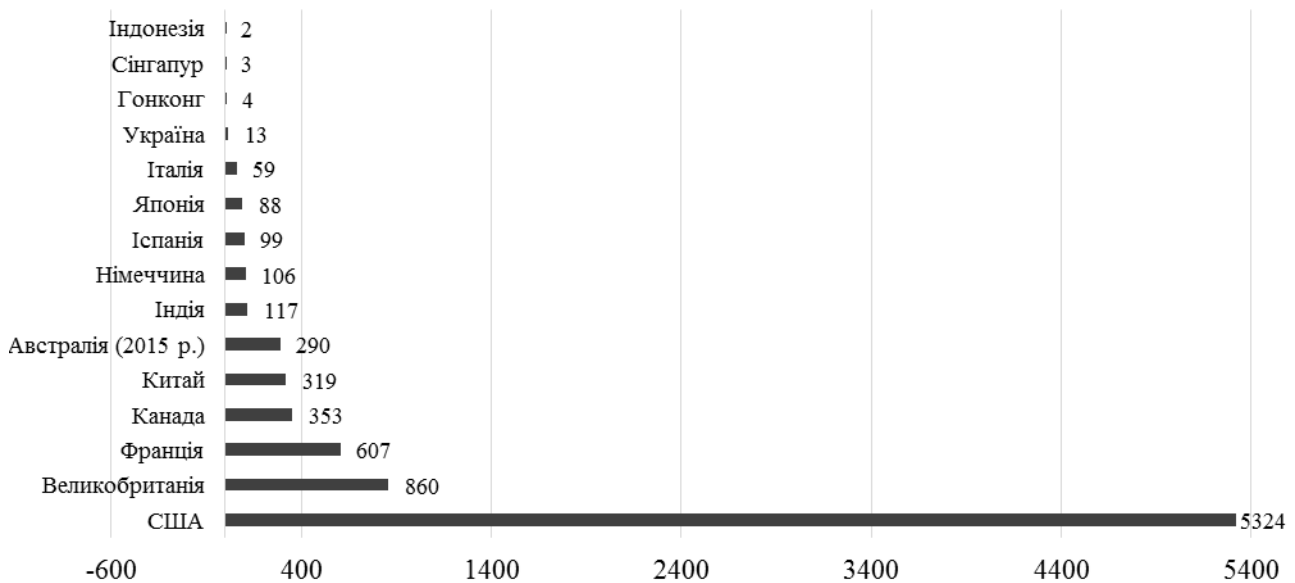
Таким чином, шахрайство у сфері банківських транзакцій можна охарактеризувати як навмисний акт бездіяльності або вчинення будь-якої дії при здійсненні банківської операції, що призводить до неправомірної вигоди для будь-якої особи за рахунок одночасного збитку для іншої особи або для банку.

Щодо характеру фінансового шахрайства, С. С. Мельник зазначає наступне: «Шахраї постійно адаптують свої маніпуляції до середовища функціонування комерційного банку та його діяльності, яка спрямована на боротьбу з фінансовим шахрайством» [3]. В результаті такої протидії знижується або нівелюється превентивна протидія, а також ускладнюється післядія (з метою здійснення рестриктивних заходів). Це тягне за собою ризики незворотньої втрати фінансових ресурсів, які є ціллю шахрайських дій.

Дослідження, представлене у даній статті, ґрунтується на статистичних даних по зафіксованих випадках транзакційного шахрайства. Отже, існує можливість похибки на об'єми незафіксованих випадків. Проте, загальні пропорції та тенденції, безумовно, зберігаються.

Для України характерні певні особливості в структурі шахрайських банківських операцій, обумовлені аспектами суспільно-економічного характеру. Вони відрізняють український банківський ринок від ринку країн, де безготівкові розрахунки розповсюджені більше, а інтернет-торгівля впевнено посуває оф-лайн формати.

На рис. 1 представлено порівняння сум шахрайських операцій в Україні та інших країнах світу.



**Рис. 1. Сумарні втрати від шахрайських операцій у 2016 р., млн. дол. США**

*Джерело: побудовано автором на основі [12; 17]*

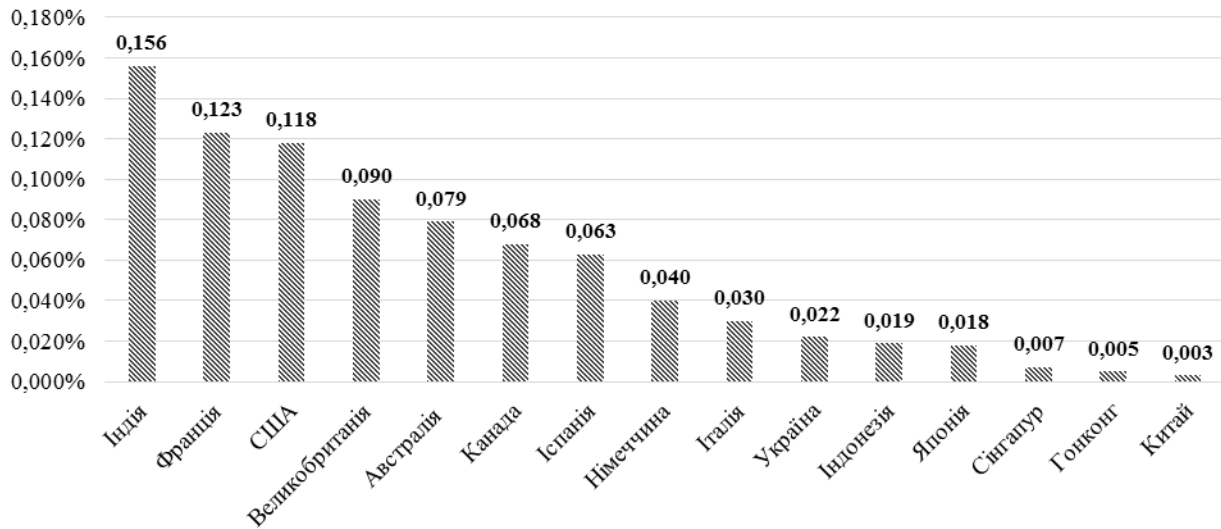
Дані рис. 1 показані в розрахунку об'єму шахрайських операцій безвідносно до загальної суми обороту по усіх транзакціях в цілому. Тому досить очікувано, що у абсолютному значенні США зазнали найвищого звітного шахрайства у розмірі 5 мільярдів доларів у 2016 році, адже саме резиденти цієї країни найбільше використовують такий інструмент, як онлайн-оплата з огляду на два фактори: чисельність населення США та його купівельну спроможність. В таких країнах Європи, як Франція та Великобританія теж спостерігається високий рівень шахрайства у платіжних операціях (\$ 607 млн. і \$ 860 млн. відповідно) [15]. В Азії значний об'єм такого роду шахрайства спостерігається в Тихоокеанському регіоні, а також у Китаї (у розмірі 319 млн. дол.) [15]. Існує чітка тенденція, яка свідчить про те, що США мають найвищий рівень шахрайства в абсолютному вимірі. Таким чином, обсяг шахрайських операцій при розрахунках залежить від загального обсягу (сум) розрахунків. Україна належить до країн з порівняно незначним обсягом безготівкових карткових розрахунків, але порівняно високим відсотком шахрайських операцій в даному сегменті.

Слід розуміти, що обсяги обумовлені загальними сумами грошового обігу, а він для різних країн відрізняється суттєво. Тому більш репрезентативним буде порівняння частки втрат від шахрайських операцій в загальному обсязі безготівкових розрахунків, яке представлено на рис. 2.

У відсотковому відношенні сум шахрайських операцій в загальному обсязі безготівкових транзакцій картина суттєво міняється [18]. «Лідером» щодо присутності шахрайських транзакцій є Індія, за якою слідують Франція, США та з деяким відривом Великобританія, Австралія, Канада. Це пов'язано, безперечно, зі ступенем захищеності транзакцій, але перш за все – з активністю зловмисників у даній сфері. Даний факт ще раз підтверджує глобальність проблеми шахрайства у банківській сфері, хоча структурні особливості такого шахрайства залежать від того, які транзакції найчастіше використовуються в тій чи іншій країні, а також від інших факторів, сприятливих для того чи іншого роду шахрайства.

З огляду на структурні особливості шахрайських операцій, цікавим буде дослідження українських реалій. Хоча, порівняно з даними по країнах, що переважають у загальних сумах втрат внаслідок

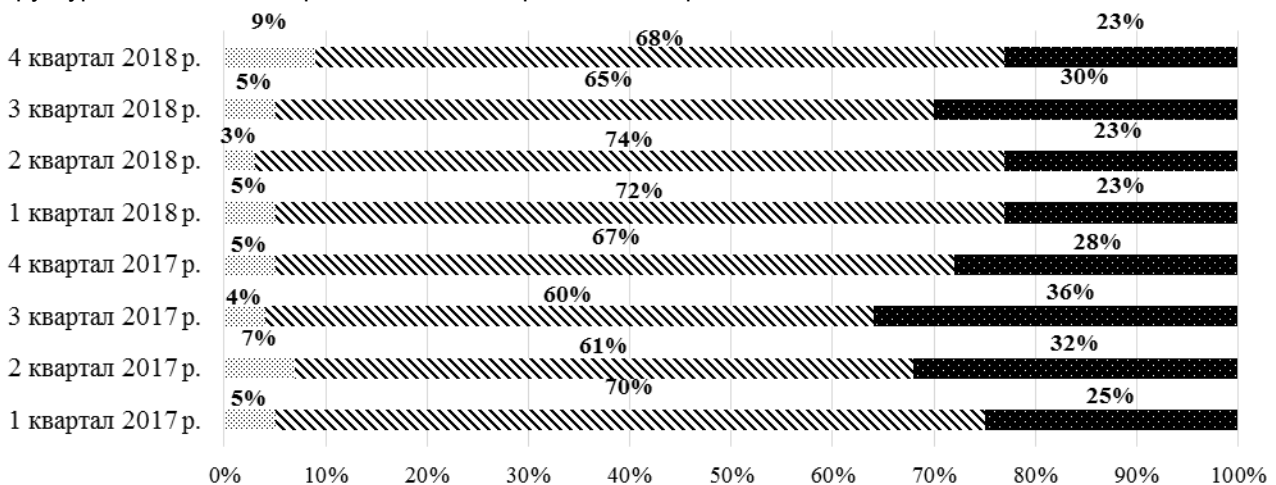
шахрайства в сегменті карткових транзакцій, українська банківська система виглядає порівняно захищеною, проте характеристики шахрайства дають уяву про найбільш проблемні напрямки транзакційного шахрайства.



**Рис. 2. Частка втрат від шахрайства у 2016 р. по відношенню до загального обсягу транзакцій, %**

Джерело: побудовано автором на основі [12]

На рис. 3 представлена структура шахрайських транзакційних операцій по платіжних картах усіх типів за 2017–2018 рр. поквартально, складена за даними Асоціації ЄМА [18]. Аналітики ЄМА об'єднали два види розповсюдженого шахрайства в один ряд даних, хоча доцільніше було б представити їх окремо. Тим не менше, на рис. 3 наочно можна спостерігати як за структурою, так і за структурною динамікою транзакційних шахрайських операцій.



☞ Дистанційне банківське обслуговування ☞ Соціальна інженерія та інтернет ■ Банкомати та POS-термінали

**Рис. 3. Структура шахрайських транзакційних операцій за період 2017–2018 рр.**

Джерело: побудовано автором на основі [14]

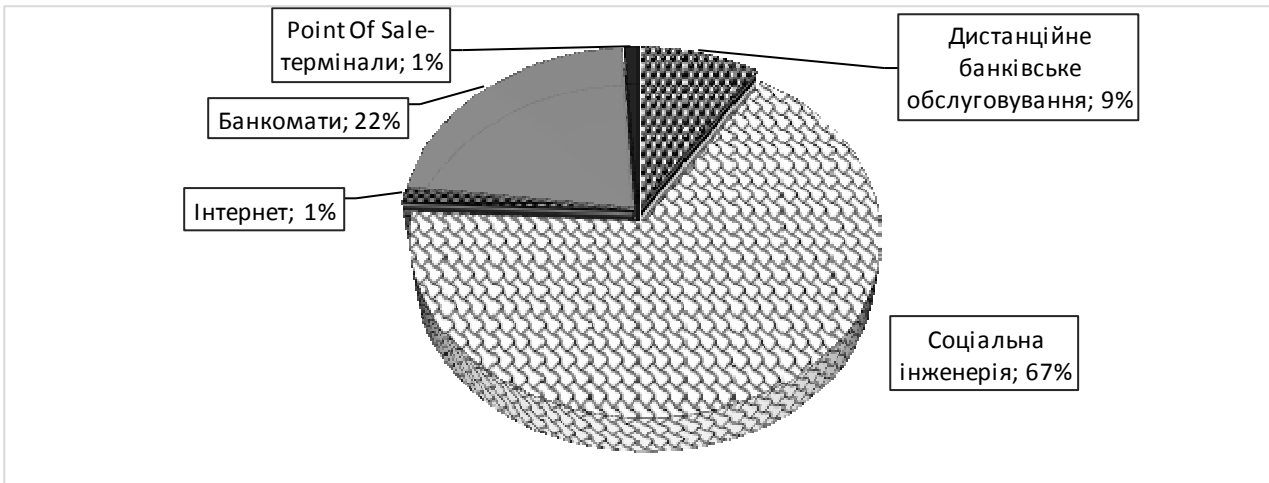
Близько 70% складають шахрайські операції, пов'язані з соціальною інженерією та проведені за допомогою мережі Інтернет. Банкоматне шахрайство складає приблизно четверту частину від усієї кількості шахрайських операцій та має тенденцію до зниження своєї частки у зв'язку з удосконаленням банківських технологій по захисту банкоматів. Значно зменшилася й до цього незначна частка шахрайських операцій через POS-термінали та дещо зростає частка випадків шахрайства при дистанційному банківському обслуговуванні.

Безумовно, залишається небезпечною проблема інтернет-шахрайства, оскільки розвиток фішингу стримують лише постійний контроль і моніторинг.

Цікаво, що інтернет-шахрайство представляє собою більш прогнозовану ділянку проблем.

На рис. 4 представлено структуру шахрайських операцій на кінець 2018 р.





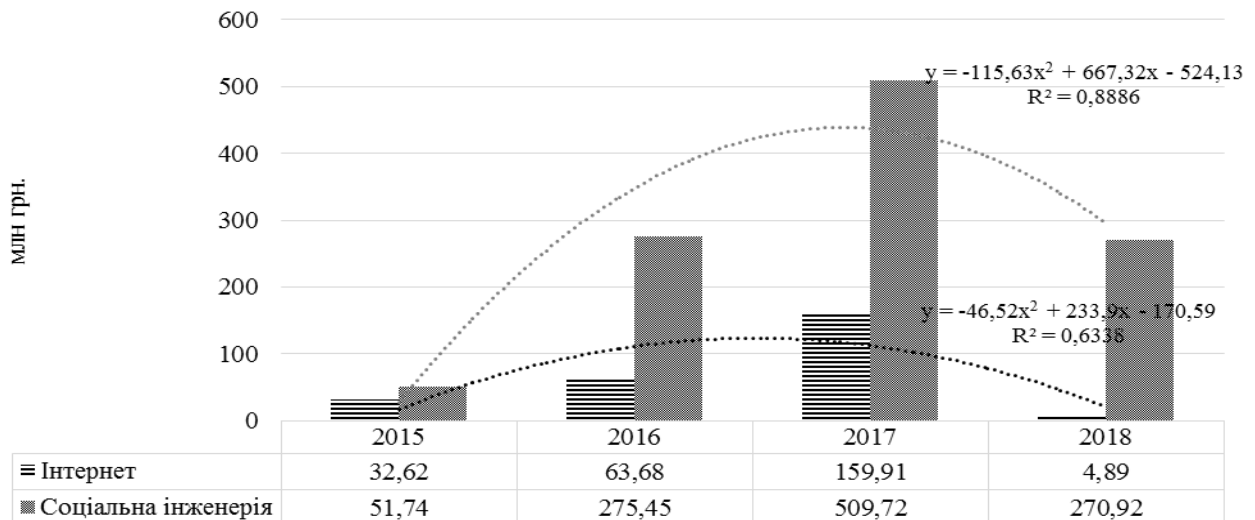
**Рис. 4. Структура обсягу шахрайських операцій на кінець 2018 р.**

Джерело: побудовано автором на основі [14]

Виходячи з аналізу ситуації з шахрайськими операціями, можна визначити, що найбільш небезпечною тенденцією є соціальна інженерія, яка на сьогодні має доволі сталу динаміку, незважаючи на постійно зростаючу кількість заблокованих виявлених телефонів зловмисників. Це пов'язано з тим, що шахрайські схеми постійно вдосконалюються, зловмисники генерують безліч різноманітних «легенд» навіть навколо приблизно однакових технологій. Окрім того, важливим фактором є така загальна тенденція, як збільшення кількості держателів платіжних карт.

Не менш небезпечною, хоча й на даний момент не настільки розповсюдженою є проблема Інтернет-шахрайства. Технологія фішингу набула найбільшого розповсюдження в 2016 р. За даними ЄМА, в українському сегменті мережі у 2016 р. функціонувало 174 фішингових сайти. Для порівняння, у 2015 р. їх було 38. У 2017 р. кількість зменшилася до 108 сайтів, а у 2018 р. – до 31. Це пов'язано як з заходами правового характеру, так і з удосконаленням банківських технологій захисту онлайн-транзакцій.

Варто відзначити, що банківський ринок в результаті постійного вдосконалення інструментарію захисту набуває резистентності проти шахрайських технологій (рис. 5).



**Рис. 5. Динаміка обсягу деяких видів шахрайських операцій**

Джерело: сформовано автором на основі [14]

Проте, суми втрат за шахрайськими операціями продовжують бути достатньо значними. Так, якщо середня сума однієї шахрайської операції в мережі Інтернет в 2018 р. складала 85 грн, то сума однієї операції за схемою соціальної інженерії – 2478 грн [14].

Як відомо, банки вдаються до комплексних, системних заходів запобігання шахрайським транзакціям. Так, ПАТ «Приватбанк» використовує скорингову модель визначення ймовірності шахрайства. Наприклад, при онлайн-оплаті будь-якою картою даного банку необхідно пройти

двоступеневу ідентифікацію (перший ступінь – реквізити карти, другий ступінь – підтвердження оплати за допомогою СМС-коду). В цілому, типова система для онлайн-банкінгу скорингова модель використовує визначення нетипових операцій за допомогою паттернів. В результаті визначені підозрілі операції піддаються більш детальному контролю і можуть бути автоматично відмінені.

Тривожним є те, що, незважаючи на усі зусилля протидії з боку правоохоронних органів (в першу чергу, кіберполіції), тенденція до зростання шахрайства з використанням соціальних технологій є явною. Посилення протидії даному виду шахрайства можливе лише за умови широкої інформаційної кампанії, направленої на максимальне висвітлення можливих шахрайських технологій, на зростання фінансової та технічної грамотності користувачів та рівня їх поінформованості про нові види шахрайських схем. Гнучкості та адаптованості зловмисників необхідно протиставити оперативне викриття шахрайських схем та доведення інформації до користувачів платіжних карт.

Щодо можливостей протидії шахрайським операціям, варто відзначити, що існує два напрямки: технічний та соціальний, в залежності від сфери застосування шахрайських технологій. Технічний шлях запобігання банківському шахрайству активно удосконалюється, постійно розвиваються технічні інструменти безпеки банківських транзакцій, розкриваються нові шахрайські схеми. Цей напрямок «приречений» на постійну еволюцію. З наведених вище даних щодо тенденцій шахрайства можна бачити, що невдовзі варто очікувати збільшення обсягу шахрайства в сфері електронної комерції. Також вкрай важливо звернути увагу на сегмент мобільних і безконтактних платежів.

Можливі заходи щодо запобігання та припинення шахрайства:

1. Удосконалювати законодавчу базу в частині мобільного зв'язку та електронного грошового обороту, в тому числі посилити відповідальність за злочини у сфері високих технологій.

2. Сформувані єдині правила для всіх операторів мобільного зв'язку з встановленням відповідальності за бездіяльність при шахрайстві з використанням обладнання або програмного забезпечення оператора.

3. Забезпечити ефективний державний нагляд за належним проведенням ідентифікації клієнтів з метою повного дотримання законодавства про ПІД / ФТ (протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, і фінансування тероризму).

4. Посилити роботу по формуванню відповідального економічної поведінки і підвищення фінансової грамотності населення, особливо в частині безпечного використання електронних засобів платежу.

Доцільним є створення єдиної інформаційної системи як єдиного сервісу для отримання інформації від операторів зв'язку. Можливості єдиної інформаційної системи:

- додаткова верифікація користувачів;
- актуалізація абонентських баз колекторських служб;
- підвищення рівня захищеності громадян – абонентів рухомого радіотелефонного зв'язку;
- підвищення рівня безпеки переказів грошових коштів з використанням мобільного телефону;
- належне виконання кредитними та іншими фінансовими організаціями нормативних вимог.

Дані переваги дають можливість звузити сферу передумов банківського шахрайства, які в сфері дистанційних платежів можуть бути такими:

- широке поширення комунікаційних пристроїв серед населення, не підготовленого до протидії шахрайству;
- використання технічних засобів для здійснення платіжних операцій в автоматичному режимі без особистої присутності власника коштів для здійснення платежу або передачі грошей іншій особі;
- рух грошових коштів на основі єдиних принципів і правил комунікації та платежів;
- недостатність заходів протидії шахраям.

Найбільш складною виглядає проблема захисту безконтактних, в тому числі «мобільних» платежів, оскільки в даному випадку основною загрозою є робота шкідливого ПО, яке здійснює втручання в платіжну систему без відома клієнта і обходячи ідентифікацію при здійсненні транзакції [4]. Тому вже сьогодні необхідним є створення відповідної нормативної бази для закріплення зон відповідальності мобільних операторів у сфері технічного забезпечення проведення фінансових транзакцій. Створивши адекватну систему запобігання шахрайства, заблокувавши можливості розсилки фішингових SMS повідомлень і можливості несанкціонованої заміни SIM карт, посиливши контроль за реалізацією контрактів мобільних операторів, можна істотно ускладнити для злочинців процес використання викрадених коштів, здійснити оперативне блокування і повернення викрадених сум.

Отже, найбільш ефективним заходом щодо протидії шахрайським операціям з боку клієнтів банків є максимальна поінформованість користувачів щодо необхідних дій в разі шахрайських атак (наприклад, психологічного тиску під час використання технологій соціальної інженерії). Також користувачі платіжних карт повинні бути повністю поінформовані щодо технічних заходів по запобіганню втрати коштів.

Превентивні заходи протидії випадкам банківського шахрайства повинні бути обов'язковими, а також мають постійно оновлюватися та доповнюватися у відповідності з розвитком технологій.

**Висновки з проведеного дослідження.** По мірі того, як фінансові установи розширюють свої цифрові послуги для задоволення зростаючих потреб клієнтів, шахраї також пристосовуються до цієї

мінливої парадигми. Якщо в Україні на даний час найбільшою небезпекою виступають шахрайські дії, пов'язані з соціальною інженерією та скіммінгом, то на найбільш розвинених технологічно банківських ринках основну небезпеку складають фішинг та хакінг, що пов'язано зі значним розповсюдженням операцій безконтактною, онлайн та мобільною оплати.

Зловмисники гнучко та оперативно пристосовуються до будь-яких можливостей і технічних умов, тому заходи превентивного характеру, покликані захистити доступ до можливостей проведення шахрайських транзакцій, є найбільш актуальним напрямком протидії шахрайству.

Побудова моделей, які дозволяють визначити потенційно небезпечні транзакції, є ефективним інструментом запобігання банківського шахрайства, який дозволяє визначити девіантні транзакції і запобігти втраті коштів клієнта.

### Література

1. Барановський О.І. Філософія безпеки: монографія, у 2 т. Київ: УБС НБУ, 2014. Т. 2: Безпека фінансових інститутів. 715 с.
2. Звіт Financial Fraud Action UK «FRAUD THE FACTS 2017 THE DEFINITIVE OVERVIEW OF PAYMENT INDUSTRY FRAUD-2017». URL: [https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud\\_the\\_facts.pdf](https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf). (дата звернення 17.05.2019).
3. Звіт CMSPI Global Fraud Trend Analysis and Review, October, 2018. URL: <https://cmspi.com/nam/resources/global-fraud-analysis/> (дата звернення 17.05.2019).
4. Звіт консалтингової компанії Stripe «Online fraud trends and behavior. December 2017» URL: <https://stripe.com/files/blog/stripe-snapshot-fraud.pdf> (дата звернення 13.05.2019).
5. Мельник С.С. Сутність фінансового шахрайства в комерційному банку. *Науковий вісник Ужгородського національного університету*. 2016. № 6, ч. 2. С. 91–95.
6. Мошенничество в банковской сфере. *Информационно-дискуссионный портал "Newsland"*. 2012. URL: <http://newsland.com/news/detail/id/916726/> (дата звернення 06.05.2019 р.).
7. Офіційний сайт Асоціації ЄМА. URL: <https://ema.com.ua> (Дата доступу: 16.05.2019 р.).
8. Офіційний сайт аналітично-консалтингової компанії SAS. URL: [https://www.sas.com/en\\_ca/](https://www.sas.com/en_ca/) (дата звернення 17.05.2019 р.).
9. Офіційний сайт аналітично-консалтингової компанії Mordor Intelligence. URL: <https://www.mordorintelligence.com/> (дата звернення 22.05.2019 р.).
10. Офіційний сайт The European Association for Secure Transactions (EAST): <https://embeddedsecuritynews.com> (дата звернення 04.05.2019 р.).
11. Поперешняк С. В. Ризики та алгоритми захисту сучасних банківських карткових технологій. *Вісник соціально-економічних досліджень*. 2013. Вип. 2, ч. 2. С. 60–67.
12. Сухонос В. П. Протидія шахрайству з фінансовими ресурсами у банківській сфері. *Кримінальне право*. 2012. № 8. С. 160–168.
13. Чернявський С.С. Фінансове шахрайство: методологічні засади розслідування: монографія. Київ: Хай-ТекПрес, 2010. 624 с.
14. Яровенко Г. М. Розробка інформаційної моделі виявлення ознак шахрайств у банках. *Економічна наука. Інвестиції: практика та досвід*. № 14/2018. С. 23-28.
15. Яровенко Г. М., Коркішко А. В. Моделювання ймовірності виникнення шахрайських операцій з кредитними картками. *Проблеми і перспективи розвитку банківської системи України*. Суми, 2015. Вип. 41. С. 237-248.
16. Яровенко Г. М., Сковронська А. І., Бояджян М. М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу. *Проблеми і перспективи розвитку банківської системи України. «Ефективна економіка»*. 2018. № 7. URL: [http://www.economy.nayka.com.ua/pdf/7\\_2018/39.pdf](http://www.economy.nayka.com.ua/pdf/7_2018/39.pdf) (дата звернення 29.04.2019 р.).
17. Яровенко Г. М., Бояджян М. М. Концептуальна модель виявлення ознак кібершахрайств в банках. *Сучасні міжнародні економічні відносини: становлення та шляхи перспективного розвитку: збірник тез наукових робіт учасників Всеукраїнської науково-практичної конференції (м. Одеса, 9-10 лютого 2018 р.)*. 2018. С. 98-100.
18. Chakrabarty K. C. Fraud in the banking sector – causes, concerns and cures. *Bank for international Settlements*. New Delhi. 2013. URL: <https://www.bis.org/review/r130730a.pdf> (дата звернення 15.05.2019).
19. D'Albore A. Card fraud losses fall to 13 year low. 2018. URL: <https://embeddedsecuritynews.com/2018/10/card-fraud-losses-fall-to-13-year-low/> (дата звернення 17.05.2019).
20. Kuznietsova N. V. Scoring Technology for Risk Assessment of Fraud in Banking. *Selected Papers of the XVI International Scientific and Practical Conference "Information Technologies and Security" (ITS 2016)*. 2016. P. 54-61.
21. Payments Trends to Watch in 2019. *ABA Banking Journal*. 2018. URL: <https://bankingjournal.aba.com/2018/11/payments-trends-to-watch-in-2019/> (дата звернення 05.05.2019).

## References

1. Baranovskyi, O.I. (2014), *Filosofia bezpeky* [The philosophy of security], monograph, UBS NBU, T. 2: Bezpeka finansovykh instytutiv, Kyiv, Ukraine, 715 p.
2. Report of Financial Fraud Action UK «FRAUD THE FACTS 2017 THE DEFINITIVE OVERVIEW OF PAYMENT INDUSTRY FRAUD-2017» (2018), available at: [https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud\\_the\\_facts.pdf](https://www.financialfraudaction.org.uk/fraudfacts17/assets/fraud_the_facts.pdf). (access date May 17, 2019).
3. Report of CMSPI Global Fraud Trend Analysis and Review, October, 2018 (2019), available at: <https://cmspi.com/nam/resources/global-fraud-analysis/> (access date May 17, 2019).
4. Report of the consulting company Stripe "Online fraud trends and behavior. December 2017" (2018), available at: <https://stripe.com/files/blog/stripe-snapshot-fraud.pdf> (access date May 13, 2019).
5. Melnyk, S.S. (2016), "The essence of financial fraud in a commercial bank", *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu*, no. 6, part 2, pp. 91–95.
6. Informatsionno-diskussionnyy portal "Newsland" (2012), "Fraud in the banking sector", available at: <http://newsland.com/news/detail/id/916726/> (access date May 06, 2019).
7. The official website of EMA, available at: <https://ema.com.ua> (access date May 16, 2019).
8. Official site of analytical and consulting company SAS, available at: [https://www.sas.com/en\\_ca/](https://www.sas.com/en_ca/) (access date May 17, 2019).
9. Official site of analytical and consulting company Mordor Intelligence, available at: <https://www.mordorintelligence.com/> (access date May 22, 2019).
10. Official website of the European Association for Secure Transactions (EAST), available at: <https://embeddedsecuritynews.com> (access date May 04, 2019).
11. Popereshniak, S.V. (2013), "Risks and algorithms for the protection of modern banking card technologies", *Visnyk sotsialno-ekonomichnykh doslidzhen*, iss. 2, part 2, pp. 60–67.
12. Sukhonos, V.P. (2012), "Fighting fraud with financial resources in the banking sector", *Kryminalne pravo*, no. 8, pp. 160–168.
13. Cherniavskiy, S.S. (2010), *Finansove shakhraistvo: metodolohichni zasady rozsliduvannia: monohrafiia* [Financial fraud: methodological principles of investigation: monograph], Khai-TekPres, Kyiv, Ukraine, 624 p.
14. Yarovenko, H.M. (2018), "Development of an information model for detecting signs of fraud in banks", *Ekonomichna nauka. Investytsii: praktyka ta dosvid*, no. 14, pp. 23-28.
15. Yarovenko, H.M. and Korkishko, A.V. (2015), "Simulation of the likelihood of fraudulent credit card transactions", *Problemy i perspektyvy rozvytku bankivskoi systemy Ukrainy*, iss. 41, pp. 237-248.
16. Yarovenko, H.M., Skovronska, A.I. and Boiadzhian, M.M. (2018), "Simulation of detection of signs of cyber threats in banks using intelligent analysis", *Problemy i perspektyvy rozvytku bankivskoi systemy Ukrainy. «Efektyvna ekonomika»*, no. 7, available at: [http://www.economy.nayka.com.ua/pdf/7\\_2018/39.pdf](http://www.economy.nayka.com.ua/pdf/7_2018/39.pdf) (access date April, 29, 2019).
17. Yarovenko, H.M. and Boiadzhian, M.M. (2018), "A conceptual model for detecting signs of cybercrime in banks", *Suchasni mizhnarodni ekonomichni vidnosyny: stanovlennia ta shliakhy perspektyvnoho rozvytku* [Modern international economic relations: formation and ways of perspective development], *Zbirnyk tez naukovykh robit uchasnykiv Vseukrainskoi naukovo-praktychnoi konferentsii* [Proceedings of the abstracts of scientific works of participants of the All-Ukrainian scientific and practical conference], Odesa, Ukraine, pp. 98-100.
18. Chakrabarty, K.C. (2013), *Fraud in the banking sector – causes, concerns and cures*. Bank for international Settlements, New Delhi, India, available at: <https://www.bis.org/review/r130730a.pdf> (access date May 15, 2019).
19. D'Albore, A. (2018), "Card fraud losses fall to 13 year low", available at: <https://embeddedsecuritynews.com/2018/10/card-fraud-losses-fall-to-13-year-low/> (access date May 17, 2019).
20. Kuznietsova, N.V. (2016), "Scoring Technology for Risk Assessment of Fraud in Banking". Selected Papers of the XVI International Scientific and Practical Conference "Information Technologies and Security", pp. 54-61.
21. Payments Trends to Watch in 2019. *ABA Banking Journal*, 2018, available at: <https://bankingjournal.aba.com/2018/11/payments-trends-to-watch-in-2019/> (access date May 05, 2019).

Стаття надійшла до редакції 26.05.2019 р.

Рецензент: канд. екон. наук, доцент Навчально-наукового інституту бізнес-технологій "УАБС" Сумського державного університету Г.М. Яровенко