

УДК 658.14/17:338.24

DOI: <https://doi.org/10.32782/business-navigator.80-50>

**Гаврилко Т.О.**

кандидат економічних наук, доцент,  
доцент кафедри фінансів, обліку та оподаткування  
*Державне некомерційне підприємство  
«Державний університет «Київський авіаційний інститут»*

**Полюхович С.С.**

здобувачка вищої освіти  
*Державне некомерційне підприємство  
«Державний університет «Київський авіаційний інститут»*

**Gavrillo Tetiana**

Candidate of Economic Sciences, Docent,  
Associate Professor at the Department of Finance,  
Accounting and Taxation  
*State Non-Commercial Company  
“State University “Kyiv Aviation Institute”*

**Poliukhovych Sofia**

Higher Education Student  
*State Non-Commercial Company  
“State University “Kyiv Aviation Institute”*

## **РИЗИКИ ФІНАНСОВОГО ШАХРАЙСТВА В УМОВАХ ЦИФРОВОГО СЕРЕДОВИЩА: МЕТОДИ ПРОТИДІЇ**

### **RISKS OF FINANCIAL FRAUD IN THE DIGITAL ENVIRONMENT: METHODS OF COUNTERACTION**

У статті досліджено загрози та виклики, пов'язані з фінансовим шахрайством в умовах стрімкого розвитку цифрових технологій. Розглянуто основні форми шахрайства, які впливають на фінансову стабільність підприємств України. Проаналізовані найбільш розповсюджені шахрайські схеми в Україні з початку повномасштабного вторгнення росії, втрати від шахрайських дій, кількість відкритих проваджень та справ, що надійшли до суду за період 2020-2024 роки. Досліджене явище банківського шахрайства як в глобальному масштабі, так і в Україні, нові форми шахрайства, що виникли внаслідок цифровізації банківських послуг. Охарактеризована сутність та приведені методи захисту від таких форм шахрайства, як фішинг, скімінг, SMS-шахрайство. Розглянуті сценарії телефонного фінансового шахрайства та загрози, що виникають внаслідок крадіжки фінансових номерів телефонів. Увагу приділено ролі превентивних заходів і цифрових інструментів моніторингу та створенню ефективної системи протидії шахрайству.

**Ключові слова:** шахрайство, фінансове шахрайство, цифрове середовище, банківські установи, методи захисту.

It has been studied in the article the threats and challenges associated with financial fraud in the context of the rapid development of digital technologies. Financial fraud in the digital era is characterized by features related to the large scale and speed of fraudulent schemes, anonymity of criminals and the predominant use of remote form for committing fraudulent acts. The development of modern technologies, the growing globalization of financial markets, and a sharp increase in the amount of client data used in financial transactions create the basis for professionalization of fraudulent schemes. The main forms of fraud that affect the financial stability of Ukrainian enterprises were considered. In the article it were analyzed the most widespread fraudulent schemes in Ukraine since the beginning of russia's full-scale invasion, losses from fraudulent actions, the number of open proceedings and cases submitted to the court in 2020-2024. The banking sector accounts for the majority of fraudulent attacks; fraudsters cause losses not only to banks and their depositors, but also negatively affect the stability of the financial system as a whole. Such crimes are characterized by high latency, as managers, fearing for the business reputation of their bank, only in rare cases file relevant statements with law enforcement agencies. It was studied the phenomenon of bank fraud both globally and in Ukraine, as well as new forms of fraud that have arisen as a result of the digitalization of banking services. The essence of fraud was characterized and methods of protection against such forms of fraud as phishing, skimming, and SMS fraud were presented. Scenarios of telephone financial fraud and threats arising from the theft of a financial phone number were considered. Attention is paid to the role of preventive measures and digital monitoring tools and the creation of an effective anti-fraud system in organizations of various types. To ensure the financial security of citizens, enterprises

and the state as a whole, their joint efforts to master and implement methods of protection against the risks of financial fraud are necessary. It is important to take into account the feasibility of an integrated approach to this phenomenon using technological, legal and educational methods to prevent and minimize threatening influences.

**Keywords:** fraud, financial fraud, digital environment, banking institutions, methods of protection.

**Постановка проблеми.** У сучасних умовах глобалізації, цифровізації та розвитку фінансових технологій проблема фінансового шахрайства набуває особливої актуальності. З кожним роком зловмисники використовують усе більш витончені методи обману, що поєднують технічні інновації з соціальним впливом. Це створює серйозні виклики як для державних інституцій, так і для бізнес-середовища, фінансових установ і пересічних громадян. Особливої гостроти проблема набуває в умовах недостатнього рівня фінансової обізнаності населення, недосконалості нормативно-правової бази та слабкої реалізації механізмів внутрішнього контролю в організаціях. Таким чином, виникає потреба у комплексному підході до дослідження фінансового шахрайства як багатовимірного явища, що охоплює правові, економічні, технологічні та соціальні аспекти, з метою розробки ефективних стратегій його попередження та протидії в умовах сучасного цифрового середовища.

**Аналіз останніх досліджень і публікацій.** Кримінальним Кодексом України визначається сутність шахрайства та приводяться умови покарання залежно від особливостей шахрайських дій [1]. Міжнародний стандарт аудиту (ISA) 240 містить визначення шахрайства та конкретизацію сутності його основних типів [2].

Дослідження заходів та способів, що дозволяють ідентифікувати і мінімізувати ризики фінансового шахрайства, здійснили Безділь Н.Б., Данилюк М.М., Дмитришин М.В. Автори класифікують різновиди фінансового шахрайства стосовно різних об'єктів (фізичні особи, підприємства, держава) та надають рекомендації щодо недопущення шахрайських дій [3].

Чекмарьова І.М. зосереджує увагу на різноманітних методах та видах шахрайства в Інтернеті, які стали розповсюдженими під час коронавірусу та воєнного стану,

пропонує способи їх попередження та обґрунтовує доцільність посилення кримінальної відповідальності за шахрайські дії під час війни [4].

Дудченко Н.В. розглядає зростання фінансового шахрайства у взаємозв'язку з розвитком цифрових технологій, приводить класифікацію фінансових злочинів та обґрунтовує доцільність застосування інструментарію попередження шахрайських дій [5].

Резнік О.М., Болгов Г.О. досліджують сутність фінансового шахрайства та пропонують стратегії, які забезпечують фінансову безпеку індивідам, підприємствам та суспільству в цілому. Авторами обґрунтовується необхідність комплексного підходу, ґрунтованого на поєднанні технічних та соціальних аспектів, для протистояння фінансовій злочинності [6].

Нежива М.О., Мисюк В.О. зосередили увагу на тенденціях розвитку шахрайства в умовах воєнного часу та сформулювали, яка роль відводиться державним діячам і чиновникам, власникам, менеджменту підприємств у протидії цьому явищу та забезпеченні стабільної економічної ситуації [7].

**Формулювання завдання дослідження.** Мета дослідження полягає у комплексному аналізі сучасного стану, особливостей прояву і основних форм фінансового шахрайства та методів виявлення і протидії шахрайським схемам.

**Виклад основного матеріалу дослідження.** У сучасному світі методи шахрайства змінюються, а вплив інформаційних технологій на життя людей стає все більш відчутним. Зростання кількості фінансових махінацій вимагає детального теоретичного дослідження цього явища. Проаналізуємо існуючі підходи науковців та законодавчу базу щодо трактування понять «шахрайство» та «фінансове шахрайство» (табл. 1).

Таблиця 1

## Підходи до розуміння сутності понять «шахрайство» та «фінансове шахрайство»

| Автор та джерело                               | Визначення поняття                                                                                                                                                                                                                                          |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Кримінальний кодекс України [1]                | Приводиться визначення шахрайства як способу привласнення чужого майна або набуття на нього права, що досягається за рахунок обманних дій чи зловживанням довірою                                                                                           |
| Міжнародний стандарт аудиту (ISA) 240 [2]      | Шахрайство розглядається як навмисне діяння, що здійснює одна або кілька осіб, які можуть бути керівниками, працівниками або третіми сторонами, використовуючи обман з метою отримати незаконну або неправомірну вигоду                                     |
| Безділь Н.Б., Данилюк М.М., Дмитришин М.В. [3] | Фінансове шахрайство розглядається як явище, що приводить до розбалансування фундаментальних економічних відносин, виникнення нечуваних збитків для національної економіки та загроз для доходів та добробуту громадян                                      |
| Чекмарьова І.М. [4]                            | Шахрайство відноситься до кримінальних правопорушень, загрожує власності окремих осіб, створює ризики ефективному функціонуванню економічної системи держави                                                                                                |
| Дудченко Н.В. [5]                              | Сутність фінансового шахрайства – у заволодінні грошима, капіталом чи завдання шкоди фінансовому стану іншим способом, використовуючи обман, вводючи в оману чи застосовуючи інші протизаконні дії                                                          |
| Резнік О.М., Болгов Г.О. [6]                   | Фінансовому шахрайству, як кримінологічній категорії та явищу, властиві ознаки, пов'язані зі сферою вчинення злочину – фінансовою сферою, специфічним суб'єктом злочинних посягань, складним механізмом злочинної поведінки                                 |
| Нежива М.О., Мисюк В.О. [7]                    | Фінансове шахрайство – явище, властиве будь-якій країні, як тій, що має розвинену економіку, так і тій, якій характерне активне становлення; чинниками, що сприяють шахрайству та ризикам злочинності у економічній сфері, є використання цифрових платформ |

Джерело: складено авторами за [1–7]

До форм фінансового шахрайства, які найчастіше використовуються, належать: нецільове використання бюджетних коштів; ухилення від сплати податків; маніпулювання фінансовою звітністю; незаконне заволодіння майном; корупція; хабарництво. Відповідно глобальних досліджень, що проводить міжнародна компанія «PricewaterhouseCoopers» (PwC), і які стосуються економічних злочинів, у 2024 році найпоширенішими в Україні були визначені [8]:

- корупція та хабарництво; 84% українських опитуваних притримуються думки, що уряду властиві стабільні або посилені дії щодо боротьби з корупцією; разом з тим, у 25% підприємств або відсутні програми управління ризиками взаємодії з третіми сторонами, або не здійснюється оцінка таких ризиків;

- шахрайські дії у сфері закупівель; 70% респондентів визнають цей вид шахрайства достатньо актуальною проблемою, однак 30% підприємств не використовують заходи для того, щоб визначити втрати із-за закупівельного шахрайства;

- шахрайства у сфері експортного контролю та санкцій; 61% опитаних відносять слідування санкціям до важливих умов діяльності підприємств; 41% відмічають ускладнення процедур контролю експорту порівняно з двома попередніми роками; 35% сподіваються на позитивний вплив на програми санкцій технологій штучного інтелекту;

- шахрайство, пов'язане з ланцюгами постачання та трудовими ризиками; 41% вітчизняних підприємств не проводився аудит для виявлення невідповідностей виконання контрагентами законодавчих вимог щодо примусової праці; 16% підприємств відносяться до оцінки таких ризиків, як до пріоритетних.

Під час війни з росією різко збільшилась кількість шахрайських дій, які привели до суттєвих збитків українських громадян. За даними спільного дослідження

Opendatabot і НБУ у 2023 році, приблизно 11% українців стали жертвами шахраїв, і більшість з них були ошукані під час продажу чи покупки в інтернеті (52,7%), за допомогою шахрайських посилань (18,6%) та злому соцмереж (12%) (рис. 1).

Кількість кримінальних проваджень, які було відкрито у 2023 році, досягло рівня 82 609, що перевищило у 2,6 рази рівень 2022 року та стало найбільшим показником за останній одинадцятирічний період. Величина втрат від шахрайських дій становила 3 млрд. грн., що втричі перевищило рівень 2022 року.

2024 рік відзначився зменшенням кількості кримінальних проваджень до 64 978 (на 21% менше за 2023 рік). Результати досліджень Rakuten Viber свідчать про те, що 62% українських громадян у 2024 році стали потерпілими із-за шахрайства з кіберпростору та телефонного шахрайства. 81% тих, хто користується Viber, контактували з інтернет-шахраями; 45% демонстрували реакцію на шахрайські посягання; 36% не реагували на такі випадки. Кількість телефонних дзвінків від шахраїв зменшилася на 80% порівняно з попереднім роком. За період січня-жовтня 2024 року шахраї здійснили дзвінки 90 000 громадянам [10].

Разом з тим, збільшилася кількість справ, що надійшли до суду, – 15 607, це склало 24% від всіх проваджень, що були відкриті у 2024 році. За попередні періоди (2022–2023 роки) ця частка знаходилася на рівні 18%. Вітчизняними судами у 2024 році було винесено 1083 вирок по справам про шахрайство; найбільшим цей показник спостерігався у 2023 році – 3100; в судовому реєстрі України зафіксовано 42 787 вироків по статті 190 ККУ «Шахрайство».

Кількість відкритих справ зменшувалося напротязі 2024 року – якщо у першому кварталі ця величина складала 8000, то за останній квартал рівень цього показника знизився до 3300 [11].

Шахрайські схеми в Україні

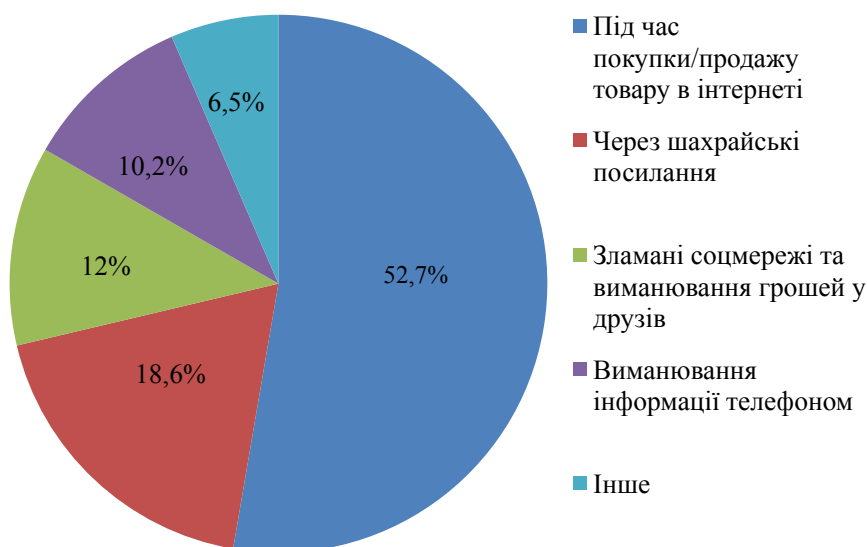


Рис. 1. Найбільш розповсюджені шахрайські схеми в Україні з початку повномасштабного вторгнення росії, %

Джерело: побудовано авторами за [9]

Дані щодо кількості відкритих проваджень та справ, що надійшли до суду за період 2020–2024 рр., представлено на рис. 2.

В умовах зростання цифрових технологій фінансове шахрайство проявляється у ряді сфер, включаючи банківську, інвестиційну, сферу страхування та інших. Значне зростання фінансового шахрайства спостерігається при здійсненні онлайн-обслуговування клієнтів.

Серед країн, де спостерігається висока поширеність шахрайства в банківському секторі, Україна посідає одне з провідних місць і входить до числа країн, де банківські платіжні операції вважаються незахищеними.

Банківські платіжні системи, які демонструють слабкий рівень захисту, можуть втратити клієнтів через ймовірність стати мішенню для шахраїв. Залучення широких верств населення до використання безготівкових операцій та ризик збитків серед них перетворює банківське шахрайство не лише на проблему банків, а й на соціальну проблему.

Величина глобальних збитків від шахрайства у банківській сфері за 2024 рік досягла 45 млрд дол. Середній збиток на один інцидент склав 4,3 млн дол.; обсяг втрат бізнесу досягнув 14 млрд дол., частка малого бізнесу у загальному обсязі втрат склала 47%. Фінансовим сектором для боротьби з шахрайством шляхом інвестування у антифрод-технології було витрачено 12,6 млрд дол., що перевищує показник попереднього року на 20%.

Втрати банківських установ України із-за шахрайських дій у 2024 році склали більше, ніж 1,7 млрд грн. Процеси «оцифрування» банківських послуг, застосування технологій штучного інтелекту спричинило появу нових форм фінансового шахрайства. Найбільшого розповсюдження набули: фішинг і вішинг, соціальна інженерія, шахрайство шляхом використання мобільних додатків, deepfake-технологій, шахрайські схеми з кредитуванням, крадіжка токенів (даних) для отримання доступу в інтернет-банкінг.

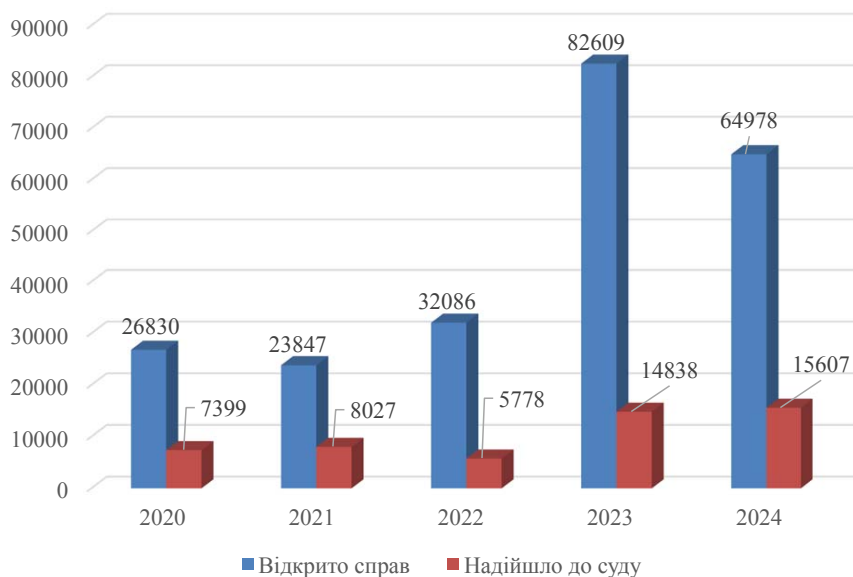
Основними формами шахрайства в Україні залишаються фішинг і соціальна інженерія, оскільки через загальну ситуацію населення країни демонструє велику вразливість. На ці дві категорії припадає майже 80% усіх випадків шахрайства, зареєстрованих в інтернет-просторі.

Фішинг – це спосіб отримання інформації про банківську картку людини за допомогою інтернет-ресурсів. Для цього зловмисники створюють копії сайтів банків, інтернет-магазинів або платіжних систем. Здійснюючи платежі на таких сайтах, жертва вводить свої банківські реквізити, що дозволяє шахраям отримати доступ до її банківського рахунку. Шахраї можуть створювати не тільки копії відомих веб-сайтів, а й абсолютно нові інтернет-ресурси. Вони часто використовують цей метод для створення інтернет-магазинів з електронікою та гаджетами, які пропонують привабливі ціни.

У 2024 році фішинг був найбільш поширеним способом реалізації кіберінцидентів, кількість яких, за інформацією CERT-UA, урядової команди реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Держслужби спецзв'язку та захисту інформації України, становила 4315 – на 69,8% більше порівняно з 2023 роком (2541 інцидентів).

За 2024 рік CERT-UA було зафіксовано 174 кіберінцидентів, за якими стоїть хакерське угруповання UAC-0006, та 277 інцидентів – від угруповання UAC-0010. За рахунок використання фішингових електронних листів розповсюджувалося шкідливе програмне забезпечення [12].

Прикладами банківських установ, які стали об'єктами фішингових кампаній, є ПриватБанк (угрупованням UAC-0006 розсилалися електронні листи зі шкідливим програмним забезпеченням SmokeLoader); попередження про фішингові електронні листи надходили клієнтам від Ощадбанку. Не афішувалася назва українського банку, база даних якого щодо 33 млн осіб була проданою [13].



**Рис. 2. Кількість відкритих проваджень та справ, що надійшли до суду за період 2020–2024 рр.**

Джерело: складено авторами за [11]

Для захисту від фішингу банківськими установами можуть бути використані наступні методи:

- двофакторна автентифікація (2FA), яка створює умови для підвищення рівня безпеки при вході в систему; за інформацією NIST, цей спосіб гарантує захист у 95% фішингових ситуацій;

- мобільні додатки з використанням біометрії – відбитків пальців, сканування обличчя (Face ID), поведінкова біометрія; частка користувачів Monobank, що застосовує Face ID або Touch ID, складає 94%; кількість клієнтів ПриватБанку, що користуються біометричним захистом, становить 6 млн чол. Лише у 0,001% випадках шахраї у банках із біометричним захистом одержують шанс на успіх;

- антифішингові фільтри – ефективні інструменти виявлення та блокування фішингових посягань ще до моменту, коли користувач може на них необдуманно відреагувати; банки можуть створювати власну систему моніторингу, залучати CERT-UA (приклад ПриватБанку); фільтрувати у месенджерах і чатах (Monobank); використовувати співпрацю з Google чи Microsoft (Ощадбанк);

- застосування кампаній по підвищенню фінансової грамотності клієнтів та навчання власних працівників щодо розпізнавання фішингових загроз. Для клієнтів можуть бути використані мобільні додатки з роз'ясненням, попередження шляхом розсилання SMS, використання соціальних мереж, організація вебінарів та онлайн-тренінгів. Для своїх працівників проводяться тренінги (72% банків), курси, загальнонаціональні кампанії (ПриватБанком у 2024 році організовано сім кампаній національного масштабу);

- використання Machine Learning-аналітики – в останні роки машинне навчання визнано фахівцями найбільш результативним для протидії фішингу. Згідно звіту компанії PYMNTS, в 2024 році зросла частка фінансових установ, що використовують AI та ML для протидії шахрайству – до 71% порівняно з 66% в 2023 році [14].

- ліміти та динамічні PIN-коди – незамінні інструменти захисту від фінансового шахрайства в умовах цифрового ландшафту. На своїх сайтах банківські установи консультують клієнтів щодо дій по встановленню або зміні інтернет-ліміту при використанні їх мобільних додатків. Приклад – сайт ПриватБанку, де розміщена інформація щодо користування послугою інтернет-ліміту у застосунку Приват-24 [15]. Банками надаються послуги по зміні PIN-кодів, наприклад, UKRSIBBANK це здійснює через додаток UKRSIB online, Ощадбанк – через банкомати або платіжні термінали;

- використання технології токенизації даних – заміна реальних карткових даних токенами (унікальними цифровими ідентифікаторами), що забезпечує захист клієнтської інформації. Платіжні сервіси Fondy, EasyPay, Google Pay або Apple Pay пропонують токенизацію банківських карток. ПриватБанком у 2016 році було запущено сервіс Visa Token Service (VTS), з участю Visa; у 2019 році почала функціонувати платформа Mastercard Digital Enablement Service for Merchants (MDES) (спільно з Mastercard та LiqPay).

Однією із схем фінансового шахрайства є скімінг. Класичний скімінг – це шахрайські пастки – приховані камери, накладні клавіатури та пристрої (скімери), які зчитують дані банківських карток. Частіше це трапля-

ється з картками, які мають лише магнітну смугу; безконтактні EMV-чип-картки володіють високою стійкістю до шахрайських посягань; дуже висока стійкість властива токенизованим карткам.

За даними НБУ, у 2024 році в Україні суттєво зросла кількість безконтактних платіжних карток – до 35 млн од., що на 14% більше 2023 року та складає 60% всіх активних платіжних карток, існуючих в країні. Кількість токенизованих платіжних карток на кінець 2024 року склала 16,5 млн од.; зростання відносно 2023 року – 33%.

Шахраями може використовуватися також безконтактний скімінг (зчитування даних на відстані); термінальний (за рахунок використання модифікованих POS-терміналів); Інтернет-скімінг (за допомогою фальшивого коду на сайті для незаконного доступу до онлайн-платежів).

Методами захисту від скімінгу можуть служити:

- використання карток з високим рівнем захисту щодо несанкціонованого доступу до даних;

- перевірка банкоматів перед здійсненням операцій та фізичний захист клавіатури;

- здійснення безконтактних платежів із застосуванням NFC, що виключає передачу реальних карткових даних;

- зміна PIN-кодів на регулярній основі;

- при проведенні онлайн-покупок переважно застосування віртуальних карток.

Поширеною схемою на сьогодні є також фінансове SMS-шахрайство (Smishing). Фінансові шахраї надсилають SMS-повідомлення з різними текстами на мобільний телефон. Таке SMS-повідомлення може інформувати особу, ніби від імені банку, про те, що картка заблокована і що необхідно терміново зателефонувати за номером, вказаним нижче. Або ж у повідомленні може бути зазначено, що з платіжної картки цієї особи перераховано певну суму фінансових коштів, і вказано номер телефону для довідок. Коли здійснюється дзвінок на даний номер, фінансові шахраї витягують одноразовий пароль, який прийде в іншому SMS-повідомленні.

Володіючи такою інформацією, фінансові шахраї можуть заволодіти коштами, що знаходяться на банківському рахунку. Повідомлення також можуть надходити від імені друга або родича з проханням позичити певну суму грошей. Фінансові шахраї отримують доступ до сторінок у соціальних мережах злочинним шляхом і надсилають повідомлення.

За даними CERT-UA, у 2024 році відбулося 60 тисяч smishing-атак, включаючи фальсифіковані кампанії ніби від таких банків, як ПриватБанк, Monobank та Ощадбанк. НБУ оприлюднив інформацію, що у 2024 році 20% випадків фішингу приходилося саме на SMS-повідомлення.

До способів захисту від SMS-шахрайства відносяться:

- не використовувати посилання з SMS та встановити на смартфоні SMS-фільтр;

- здійснювати контроль надісланих реквізитів;

- користуватися банківськими застосунками, які є більш безпечними порівняно з іншими способами комунікації;

- інформувати банківську установу і CERT-UA про шахрайські SMS-повідомлення.

Телефонне фінансове шахрайство відноситься до найпоширеніших видів соціальної інженерії. Фінансовий злочинець телефонує та переконує особу надати особисту, фінансову або конфіденційну інформацію або переказати фінансові ресурси. Метою фінансових шахраїв є з'ясування реквізитів карток, паролів та SMS-кодів у банків та мобільних операторів. Ознаками телефонної розмови з фінансовим шахраєм є тривожна ситуація для особи, психологічний тиск з боку співрозмовника та поспіх.

Сценарії телефонного фінансового шахрайства можуть бути різноманітними. Наприклад, особі повідомляють, що вона виграла велику суму грошей, але для її отримання їй потрібно переказати комісію на інший банківський рахунок тощо. Або фінансовий шахрай видає себе за представника служби безпеки банку. Він повідомляє про кібератаку на IT-систему банку, запевняє, що намагаються все виправити та взяти ситуацію під контроль, але для того, щоб фінансові ресурси особи були в безпеці, їх потрібно перевести на тимчасовий резервний рахунок.

Жертвою фінансових телефонних шахраїв може стати особа, яка хоче продати певне майно через Інтернет. Фінансові шахраї запевняють продавця, що здійснять безготівковий платіж на банківську картку, та дізнаються від особи необхідну інформацію (номер картки та одноразовий пароль). Зазвичай такі телефонні дзвінки здійснюються вранці, в кінці робочого дня або робочого тижня, коли людина виснажена, втомлена та не така зосереджена, почуття притуплені, пам'ять, увага та сприйняття інформації не такі добрі. Розмова ведеться у стані нервової напруги, що бентежить.

Відповідно даних Кіберполіції, 38% випадків фінансового шахрайства у 2024 році були здійснені шляхом телефонних дзвінків; величина середніх втрат на одну особу складала у межах 5000–25000 грн, хоча траплялися випадки збитків до 500 000 грн.

Способами захисту від телефонного шахрайства можуть бути:

- збереження конфіденційності реквізитів картки та використання лише офіційних каналів зв'язку;
- застосування додатків із захистом від шахраїв;
- блокування підозрілих телефонних номерів;
- підтримка інформованості про створення нових шахрайських схем.

Крадіжка фінансового номера телефону створює надзвичайно загрозливу ситуацію із-за прив'язки до банківських рахунків. На нього надсилаються всі коди для підтвердження транзакцій, паролі від банків та інформація про залишок коштів на рахунках. Фінансові шахраї двічі поповнюють фінансовий номер телефону фізичної особи на невелику суму, телефонують особі та кладуть слухавку. Маючи інформацію про останні суми поповнення фінансового номера телефону та номер останнього вхідного дзвінка, фінансові шахраї відновлюють SIM-картку як втрачену та стають власниками фінансового номера телефону фізичної особи.

Таким чином, фінансовий шахрай має доступ до інтернет-банкінгу та одноразових паролів. За допомогою цієї схеми фінансового шахрайства середня сума

викрадених фінансових коштів з банківських рахунків фізичних осіб зросла в 2024 році до 50–150 тис. грн; в 2022 році вона складала 15–25 тис. грн.

Методами захисту можуть бути:

- використання PIN-коду для SIM-карти;
- заборона дистанційної заміни SIM-карти;
- застосування двофакторної автентифікації;
- не оприлюднення фінансового номера телефону в соціальних мережах.

Фінансове шахрайство у сфері інтернет-шопінгу – фізична особа передає фінансові ресурси фінансовим шахраям, але не отримує товар. Псевдо продавцями зазвичай використовуються достатньо відомі прийоми, які свідчать про шахрайські наміри і на які покупець повинен звертати увагу перед прийняттям рішення про придбання товару. Зазвичай це нижча ціна на товар, порівняно із пропозиціями інших продавців, стислі строки для здійснення оплати, недостатня інформація про товар, нездатність продавця дати вичерпну характеристику товару, переадресація з сайту на месенджер для листування.

Кіберполіцією у 2024 році було одержано 22000 скарг щодо шахрайства в онлайн-торгівлі; величина втрат склала 440 млн. грн.; для шахрайських схем використовувалися частіше всього OLX, Facebook Marketplace, Instagram-магазини.

Способи захисту:

- вибір відомих офіційних маркетплейсів;
- здійснення оплати лише після перевірки товару на пошти;
- не переходити по посиланням в соціальних мережах;
- встановити повідомлення про кожну здійснювану транзакцію.

**Висновки.** Фінансовому шахрайству в умовах цифрової епохи властиві особливості, пов'язані з великими масштабами та швидкістю здійснення шахрайських схем, анонімністю злочинців та переважним застосуванням дистанційної форми для скоєння шахрайських дій. Розвиток сучасних технологій, зростання процесів глобалізації фінансових ринків, різке збільшення об'єму використовуваних у фінансових операціях клієнтських даних створює базу для професіоналізації шахрайських схем.

Пріоритетною сферою шахрайських посягань є банківський сектор; результати шахрайства не лише шкодять фінансовому стану банківських установ та їх клієнтам, а і впливають на довіру громадян до фінансової системи країни. Для таких злочинів характерна висока латентність, пов'язана з небажанням топ-менеджменту банків афішувати скоєні шахрайські дії, виходячи з того, що звернення у правоохоронні органи може погіршити імідж установи, зменшити клієнтську базу та надати переваги конкурентам.

Для забезпечення фінансової безпеки громадян, підприємств та держави в цілому необхідні їх спільні зусилля по оволодінню та реалізації методів захисту від ризиків фінансового шахрайства. Важливим є урахування доцільності комплексного підходу до цього явища з використанням технологічних, правових та освітніх способів попередження та мінімізації загрозливих впливів.

### Список використаних джерел:

1. Кримінальний кодекс України: Закон України від 05 квітня 2001 року № 2314ІІІ. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 02.05.2025).

2. International standard on auditing 240 the auditor's responsibilities relating to fraud in an audit of financial statements. URL: <https://chrome-extension://efaidnbmnnnibpcajpcgclefind> (дата звернення: 02.05.2025).
3. Безділ Н.Б., Данилюк М.М., Дмитришин М.В. Ідентифікація та мінімізація ризиків фінансового шахрайства під час прийняття управлінських рішень. *Економіка та суспільство*. 2024. Вип.64. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/4289/4214> (дата звернення: 02.05.2025).
4. Чекарьова І.М. Шахрайство в інтернеті як один із видів шахрайства. *Аналітично-порівняльне правознавство*. 2024. № 2. С. 639–643.
5. Дудченко Н.В. Світові тенденції фінансового шахрайства. *Цифрова економіка та економічна безпека*. 2023. Вип. 5(05). С. 86–92.
6. Резнік О.М., Болгов Г.О. Фінансове шахрайство: сутність та заходи протидії. *Юридичний науковий електронний журнал*. 2023. № 11. С. 502–505.
7. Нежива М.О., Мисюк В.О. Протидія шахрайству в умовах війни. *Бізнесінформ*. 2023. № 1. С. 160–166.
8. PwC Global Economic Crime Survey 2024. URL: [https://www.pwc.com/ua/en/survey/2024/global-economic-crime-survey.html?utm\\_source=chatgpt.com](https://www.pwc.com/ua/en/survey/2024/global-economic-crime-survey.html?utm_source=chatgpt.com) (дата звернення: 04.05.2025).
9. Жертвами фінансових шахраїв від початку війни став кожен 9-й – опитування НБУ. URL: [https://interfax.com.ua/news/general/940167.html?utm\\_source=chatgpt.com](https://interfax.com.ua/news/general/940167.html?utm_source=chatgpt.com) (дата звернення: 04.05.2025).
10. Кількість телефонного шахрайства скоротилась на 80% – опитування. Міністерство фінансів. URL: [https://minfin.com.ua/ua/2024/11/18/140043629/?utm\\_source=chatgpt.com](https://minfin.com.ua/ua/2024/11/18/140043629/?utm_source=chatgpt.com) (дата звернення: 04.05.2025).
11. В Україні відкрили майже 65 тисяч проваджень про шахрайство: резонансні справи на півдні країни. URL: [https://intent.press/news/society/2025/v-ukrayini-vsdrili-maije-65-tisyach-provadgen-pro-shahraystvo-rezonansni-spravi-na-pivdni-krayini/?utm\\_source=chatgpt.com](https://intent.press/news/society/2025/v-ukrayini-vsdrili-maije-65-tisyach-provadgen-pro-shahraystvo-rezonansni-spravi-na-pivdni-krayini/?utm_source=chatgpt.com) (дата звернення: 04.05.2025).
12. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. 2024. Річний звіт. URL: <https://chrome-extension://efaidnbmnnnibpcajpcgclefind> (дата звернення: 05.05.2025).
13. 33 Million Ukrainian Bank Database Allegedly Leaked. URL: [https://cyberpress.org/ukrainian-bank-database-leaked/?utm\\_source=chatgpt.com](https://cyberpress.org/ukrainian-bank-database-leaked/?utm_source=chatgpt.com) (дата звернення: 05.05.2025).
14. 71% of Financial Institutions Turn to AI to Fight Faster Payments Fraud. URL: <https://www.pymnts.com/fraud-prevention/2024/71-percent-of-financial-institutions-turn-to-ai-to-fight-faster-payments-fraud/> (дата звернення: 06.05.2025).
15. Що таке інтернет-ліміт? URL: [https://privatbank.ua/handbook/internet-limit-yak-pratsiuie?utm\\_source=chatgpt.com](https://privatbank.ua/handbook/internet-limit-yak-pratsiuie?utm_source=chatgpt.com) (дата звернення: 06.05.2025).

### References:

1. Kryminal'nyy kodeks Ukrayiny: Zakon Ukrayiny vid 05 kvitnya 2001 roku № 2314III [Criminal Code of Ukraine: Law of Ukraine No. 2314 III dated April 5, 2001]. Available at: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (accessed May 2, 2025).
2. International standard on auditing 240 the auditor's responsibilities relating to fraud in an audit of financial statements. Available at: <https://chrome-extension://efaidnbmnnnibpcajpcgclefind> (accessed May 2, 2025).
3. Bezdil N. B., Danylyuk M. M., Dmytryshyn M. V. (2024) Identyfikatsiya ta minimizatsiya ryzykiv finansovoho shakhraystva pid chas pryynyattya upravlins'kykh rishen' [Identification and minimization of financial fraud risks when making management decisions]. *Economy and Society*, vol. 64. Available at: <https://economyandsociety.in.ua/index.php/journal/article/view/4289/4214> (accessed May 2, 2025).
4. Chekmareva I. M. (2024) Shakhraystvo v interneti yak odyin iz vydiv shakhraystva [Internet fraud as one of the types of fraud]. *Analytical and comparative law*, no. 2, pp. 639 – 643.
5. Dudchenko N. V. (2023) Svitovi tendentsiyi finansovoho shakhraystva [World trends in financial fraud]. *Digital economy and economic security*, no. 5(05), pp. 86–92.
6. Ryznyk O. M., Bolhov H. O. (2023) Finansove shakhraystvo: sutnist' ta zakhody protydyi [Financial fraud: essence and countermeasures]. *Legal scientific electronic journal*, no. 11, pp. 502–505.
7. Nezhyva M. O., Mysyuk V. O. (2023) Prottydiya shakhraystvu v umovakh viyny [Counteracting fraud in wartime]. *Businessinform*, no. 1, pp. 160 – 166.
8. PwC Global Economic Crime Survey 2024. Available at: [https://www.pwc.com/ua/en/survey/2024/global-economic-crime-survey.html?utm\\_source=chatgpt.com](https://www.pwc.com/ua/en/survey/2024/global-economic-crime-survey.html?utm_source=chatgpt.com) (accessed May 4, 2025).
9. Zhertvamy finansovykh shakhrayiv vid pochatku viyny stav kozhen 9-y – opytuvannya NBU [Every 9th person has become a victim of financial fraud since the beginning of the war – NBU survey]. Available at: [https://interfax.com.ua/news/general/940167.html?utm\\_source=chatgpt.com](https://interfax.com.ua/news/general/940167.html?utm_source=chatgpt.com) (accessed May 4, 2025).
10. Kil'kist' telefonnoho shakhraystva skorotylas' na 80% — opytuvannya. Ministerstvo finansiv [The number of telephone frauds has decreased by 80% – survey. Ministry of Finance]. Available at: [https://minfin.com.ua/ua/2024/11/18/140043629/?utm\\_source=chatgpt.com](https://minfin.com.ua/ua/2024/11/18/140043629/?utm_source=chatgpt.com) (accessed May 4, 2025).
11. V Ukrayini vidkryly mayzhe 65 tysyach provadzen' pro shakhraystvo: rezonansni spravy na pivdni krayiny [Almost 65 thousand fraud cases opened in Ukraine: high-profile cases in the south of the country]. Available at: [https://intent.press/news/society/2025/v-ukrayini-vsdrili-maije-65-tisyach-provadgen-pro-shahraystvo-rezonansni-spravi-na-pivdni-krayini/?utm\\_source=chatgpt.com](https://intent.press/news/society/2025/v-ukrayini-vsdrili-maije-65-tisyach-provadgen-pro-shahraystvo-rezonansni-spravi-na-pivdni-krayini/?utm_source=chatgpt.com) (accessed May 4, 2025).
12. Systemy vyavleniya vrazlyvostey i reahuvannya na kiberintsyenty ta kiberatomy. 2024. Richnyy zvit [Vulnerability Detection and Response Systems for Cyber Incidents and Cyberattacks. 2024. Annual Report]. Available at: <https://chrome-extension://efaidnbmnnnibpcajpcgclefind> (accessed May 5, 2025).
13. 33 Million Ukrainian Bank Database Allegedly Leaked [33 Million Ukrainian Bank Database Allegedly Leaked]. Available at: [https://cyberpress.org/ukrainian-bank-database-leaked/?utm\\_source=chatgpt.com](https://cyberpress.org/ukrainian-bank-database-leaked/?utm_source=chatgpt.com) (accessed May 5, 2025).
14. 71% of Financial Institutions Turn to AI to Fight Faster Payments Fraud. Available at: <https://www.pymnts.com/fraud-prevention/2024/71-percent-of-financial-institutions-turn-to-ai-to-fight-faster-payments-fraud/> (accessed May 6, 2025).
15. Shcho take internet-limit? [What is an internet limit?] Available at: [https://privatbank.ua/handbook/internet-limit-yak-pratsiuie?utm\\_source=chatgpt.com](https://privatbank.ua/handbook/internet-limit-yak-pratsiuie?utm_source=chatgpt.com) (accessed May 6, 2025).