

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ УПРАВЛІННЯ,
ПСИХОЛОГІЇ ТА БЕЗПЕКИ

Кафедра менеджменту та економічної безпеки

ПРОТИДІЯ ФІНАНСОВОМУ ШАХРАЙСТВУ В УКРАЇНІ

кваліфікаційна робота
здобувач вищої освіти
2 курсу заочної форми навчання
ЖИГАЙЛО Назар Романович

Науковий керівник
кандидат економічних наук, доцент
НАГІРНА Оксана Вікторівна

Рецензент
доктор економічних наук, професор
МИСЬКІВ Галина Василівна

Кваліфікаційна робота допущена до захисту

« » 2025 р., протокол №
завідувач кафедри менеджменту
та економічної безпеки

_____ **КОПИТКО М. І.**

Львів
2025

АНОТАЦІЯ

ЖИГАЙЛО Н.Р. Протидія фінансовому шахрайству в Україні. - Рукопис.

Кваліфікаційна робота на здобуття освітнього ступеня «магістр» за спеціальністю 072 «Фінанси, банківська справа, страхування та фондовий ринок». - Львівський державний університет внутрішніх справ МВС України, Львів, 2025.

У рамках кваліфікаційної роботи було досліджено поняття «фінансове шахрайство» та визначено ключові фактори, які сприяють його поширенню. Проведено систематизацію основних ризиків, пов'язаних із фінансовим шахрайством, а також проаналізовано механізми державного регулювання, спрямовані на боротьбу з такими правопорушеннями. Вивчено поширені схеми фінансового шахрайства та оцінено їхній вплив і масштаби на території України. Крім того, узагальнено міжнародний досвід у сфері запобігання шахрайським діям і запропоновано стратегічні кроки для посилення протидії фінансовим махінаціям.

Ключові слова: фінансове шахрайство, шахрайські схеми, заходи протидії фінансовому шахрайству, фінансові втрати, незаконна операція, міжнародний досвід, державна політика.

ANNOTATION

ZHYGAILO N.R. Counteracting Financial Fraud in Ukraine. - Manuscript.

Qualification thesis for obtaining the Master's degree in specialty 072 "Finance, Banking, Insurance, and Stock Market." - Lviv State University of Internal Affairs of the Ministry of Internal Affairs of Ukraine, Lviv, 2025.

This qualification thesis explores the concept of "financial fraud" and identifies key factors contributing to its spread. The study systematizes the main risks associated with financial fraud and analyzes state regulatory mechanisms aimed at combating such offenses. Common financial fraud schemes are examined, assessing their impact and scale within Ukraine. Additionally, international experience in fraud prevention is summarized, and strategic measures are proposed to strengthen efforts against financial manipulations.

Keywords: financial fraud, fraudulent schemes, measures to counter financial fraud, financial losses, illegal transactions, international experience, state policy.

ЗМІСТ

ВСТУП.....	4
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ПРОТИДІЇ ФІНАНСОВОГО ШАХРАЙСТВА	7
1.1. Фінансове шахрайство: економічна сутність та чинники поширення	7
1.2. Ідентифікація та мінімізація ризиків фінансового шахрайства.....	12
1.3. Державне регулювання протидії фінансовому шахрайству.....	17
Висновки до розділу 1	23
РОЗДІЛ 2. ОЦІНКА РЕЗУЛЬТАТИВНОСТІ ПРОТИДІЇ ФІНАНСОВОМУ ШАХРАЙСТВУ	24
2.1. Типові схеми виявлення фінансового шахрайства.....	24
2.2. Аналіз рівня поширення фінансового шахрайства та ефективності заходів щодо його протидії.....	32
Висновки до розділу 2.....	39
РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ ЗАХОДІВ ПРОТИДІЇ ФІНАНСОВОМУ ШАХРАЙСТВУ В СУЧАСНИХ УМОВАХ.....	40
3.1. Міжнародний досвід у сфері боротьби з фінансовим шахрайством та перспективи його застосування в Україні.....	40
3.2. Вдосконалення державної політики у сфері протидії фінансовому шахрайству	48
Висновки до розділу 3.....	55
ВИСНОВКИ	56
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	59

ВСТУП

Актуальність теми дослідження. На сучасному етапі розвитку науки та технологій проблема фінансового шахрайства стає дедалі актуальнішою. Технологічний прогрес, цифровізація та інновації загалом відкривають перед людством значні можливості для покращення якості життя та розвитку суспільства. Проте, поряд із позитивними змінами, вони створюють умови для появи нових шахрайських схем і махінацій. Будь-який розвиток має дві сторони – позитивну і негативну, і фінансове шахрайство є одним із небажаних наслідків технологічного прогресу.

Шахрайські дії дедалі активніше проникають у різні сфери людської діяльності, створюючи серйозні ризики для стабільності та розвитку суспільства. Фінансові махінації можуть бути спрямовані як на бізнес-суб'єкти, так і на звичайних громадян. Головною рушійною силою шахраїв залишається корисливий інтерес, незалежно від того, яку саме схему обману вони використовують.

Порівняно зі звичайною крадіжкою, фінансове шахрайство вирізняється більш прихованими методами заволодіння грошима. Щороку з'являються нові види шахрайських схем, які адаптуються до сучасних технологій, створюючи нові виклики для суспільства.

У сучасних умовах фінансове шахрайство все частіше набуває інтелектуального характеру, оскільки зловмисники не лише використовують новітні технології, але й активно застосовують сучасні психологічні методики впливу. Аналізуючи види фінансових махінацій, зокрема ті, що стосуються підприємств, можна дійти висновку, що такі дії несуть значні ризики не лише для репутації організації, але й для її фінансової стабільності загалом. Тому дослідження особливостей сучасного фінансового шахрайства, його виявлення та розробка ефективних заходів протидії є надзвичайно важливими на сьогодні.

Проблематика протидії фінансовому шахрайству привернула увагу багатьох видатних науковців. Вагомий внесок у вивчення цієї теми зробили такі дослідники, як Є. А. Абрамєйцева, М. М. Данилюк, М. В. Дмитришин, Т. О. Кізима, І. О. Коновалова, О. В. Кравченко, О. Г. Мельник, В. О. Мисюк, Т. О. Мудряк, М. О. Нежива, В. В. Сухонос, Ю. Я. Хамига, Г. М. Чернишов, С. С. Чернявський, С. П. Чорнуцький та інші.

У кваліфікаційній роботі були застосовані наукові праці українських та зарубіжних авторів, що стосуються теми дослідження, а також нормативно-правові акти України, дані від правоохоронних органів і фінансових установ.

Мета і завдання дослідження. Метою цієї кваліфікаційної роботи є визначення теоретичних і практичних підходів до протидії фінансовому шахрайству. Для досягнення поставленої мети у роботі виконувалися такі завдання:

- визначити сутність поняття «фінансове шахрайство» та чинники, які сприяють його розповсюдженню;
- систематизувати існуючі види ризиків фінансового шахрайства;
- вивчити механізми державного управління у сфері протидії фінансовим махінаціям;
- дослідити основні типи фінансових шахрайських схем;
- оцінити масштаби фінансового шахрайства на території України;
- узагальнити досвід інших країн у сфері запобігання фінансовому шахрайству;
- запропонувати стратегічні заходи для протидії фінансовому шахрайству.

Об'єктом дослідження є фінансові операції ключових суб'єктів економіки.

Предметом дослідження є підходи, інструменти та заходи, спрямовані на запобігання фінансовому шахрайству.

Методи дослідження. Для реалізації поставлених завдань було використано комплекс наукових методів і прийомів, які забезпечили всебічне

вивчення об'єкта дослідження. Методи формальної логіки, такі як аналіз, синтез, дедукція, індукція, аналогія та абстрагування, сприяли деталізації змісту питань, що розглядалися у всіх розділах кваліфікаційної роботи.

Наукова новизна. Результати, отримані в рамках кваліфікаційної роботи, можуть стати основою для використання державними органами під час формування та вдосконалення заходів, спрямованих на запобігання і протидію фінансовим махінаціям.

Основний зміст роботи. Кваліфікаційна робота включає вступ, три основні розділи, підсумкові висновки та перелік використаних джерел.

У першому розділі досліджуються: сутність поняття «фінансове шахрайство»; фактори, що впливають на його розповсюдження; основні ризики фінансового шахрайства; інструменти державного регулювання для запобігання та боротьби з фінансовим шахрайством.

Другий розділ присвячений аналізу типових схем виявлення фінансового шахрайства і оцінці масштабів його поширення.

У третьому розділі вивчається міжнародний досвід боротьби з фінансовими шахрайствами, а також розробляються основні рекомендації щодо протидії цьому явищу в Україні.

Структура роботи. У кваліфікаційній роботі представлено вступ, три ключові розділи, висновки та бібліографію. Загальний обсяг роботи становить 64 сторінки, з яких основний текст займає 55 сторінок. Робота містить дві таблиці та сім рисунків. Список літератури нараховує 54 позиції.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ПРОТИДІЇ ФІНАНСОВОГО ШАХРАЙСТВА

1.1. Фінансове шахрайство: економічна сутність та чинники поширення

На сучасному етапі розвитку науки і технологій проблема шахрайства набуває дедалі більшої актуальності. Хоча науково-технічний прогрес відіграє важливу роль у поліпшенні якості життя, він водночас сприяє розвитку негативних явищ, зокрема шахрайства, яке швидко проникає в усі сфери суспільного життя. Це явище становить серйозну загрозу для стабільного функціонування і розвитку людства.

Фінансове шахрайство, яке зачіпає як майно, так і кошти громадян та підприємств, має на меті отримання неправомірної вигоди. На відміну від традиційних форм крадіжки, воно передбачає заволодіння чужими фінансовими ресурсами прихованими способами. Зловмисники керуються корисливими мотивами, застосовуючи різноманітні схеми обману.

Щороку виникають нові види шахрайства, а розвиток технологій сприяє їх адаптації до сучасних умов. У наш час шахрайство стає дедалі витонченішим, оскільки злочинці використовують не лише інноваційні технологічні рішення, а й сучасні психологічні методи, що робить це явище особливо небезпечним.

Дослідження шахрайства та розробка методів боротьби з ним завжди перебували у центрі уваги науковців, про що свідчить значна кількість присвячених цій темі праць. Водночас термін "шахрайство" трактується по-різному в роботах різних дослідників, що відображає різноманітність підходів до його визначення.

Згідно з Тлумачним словником української мови, поняття "шахрайство" визначається як «хитрий та винахідливий обман; хитрощі, ошуканство». У

науковій літературі це слово часто вживається зі синонімами, такими як «афера», що означає ризиковану діяльність із метою збагачення, або «махінація», яка передбачає застосування хитрощів для досягнення певної мети [30, с. 423].

Відповідно до положень Міжнародного стандарту аудиту (ISA) 240, шахрайство визначається як умисні дії, вчинені однією чи кількома особами з числа керівників, працівників або сторонніх осіб, які здійснюються шляхом обману з метою отримання незаконної або неправомірної вигоди [51].

О. Кравченко у своєму дослідженні робить висновок, що шахрайство належить до категорії злочинів, які часто відбуваються за активної або несвідомої участі потерпілого. На його думку, шахрайство завжди є наслідком взаємодії трьох ключових чинників: специфічної криміногенної ситуації, дій злочинця та поведінки жертви [13].

Ю. Хамига визначає фінансове шахрайство як сукупність економічних взаємовідносин, які здійснюються фізичними чи юридичними особами (зазвичай без застосування насильства) у процесі формування, розподілу та використання фінансових ресурсів. При цьому використовуються обман, зловживання довірою чи службовим становищем для досягнення економічної або іншої вигоди, що може бути особистою, корпоративною або в інтересах третіх осіб [39, с. 23].

У контексті наукового підходу, наприклад, український дослідник С. Чорнуцький визначає фінансове шахрайство як злочин, пов'язаний із порушенням встановлених законодавством України правил фінансування, кредитування та оподаткування підприємницької діяльності. Фінансове шахрайство він трактує як навмисні дії фізичної або юридичної особи чи групи осіб, які порушують вимоги чинного законодавства України задля отримання доходів, матеріальних благ тощо [42, с. 128].

О. Чумаченко пропонує розглядати шахрайство як умисне заволодіння чужим майном або отримання права на нього через обман чи зловживання довірою, що завдає економічних збитків потерпілій стороні та/або приносить

економічну вигоду злочинцю [4]. Таке трактування розширює розуміння цієї категорії, акцентуючи увагу на отриманні злочинцем вигідних економічних наслідків. Згідно з положеннями Міжнародного стандарту аудиту (ISA), шахрайство визначається як умисні дії однієї або кількох осіб із числа керівників, управлінського персоналу, працівників чи сторонніх осіб, спрямовані на використання обману для здобуття незаконної або неправомірної вигоди [51]. Це визначення підкреслює наявність спеціального суб'єкта - службової особи, яка діє в особистих інтересах. Усі визначення шахрайства об'єднує головний спосіб його вчинення - обман, що й відрізняє це правопорушення від інших.

Г. Чернишов у своїх дослідженнях трактує фінансове шахрайство як форму злочинної діяльності. Він визначає таку діяльність як деструктивну та протиправну поведінку, яка характеризується свідомими, мотивованими діями, спрямованими на досягнення певної мети чи задоволення потреб. Ці дії можуть бути як законними, так і незаконними, проте вони завжди є умисними та мотивованими [40].

В. Сухонос вказує, що шахрайство у фінансовій сфері, особливо в банківській галузі, часто пов'язане з організованою злочинністю. Така злочинність може проникати в державні установи, правоохоронні органи, банківські та небанківські фінансові установи для отримання доступу до необхідної інформації та забезпечення захисту своїх дій. Дослідник підкреслює, що для ефективної боротьби з шахрайством потрібен системний і збалансований підхід держави, спрямований на захист фінансових інтересів банків, юридичних і фізичних осіб, а також самої держави від економічних злочинів у банківській сфері [32].

Міжнародна аудиторська компанія «PricewaterhouseCoopers» (надалі – PwC) активно досліджує питання шахрайства, зокрема з метою проведення статистичних аналізів. Згідно зі звітом "Всесвітнє дослідження економічних злочинів та шахрайства 2020 року", ця проблема є поширеною у нашій країні. Близько половини опитаних респондентів заявили, що зазнали впливу

економічних злочинів та шахрайських дій. Компанії оцінюють збитки від таких випадків у понад 100 тисяч доларів, при цьому зазначають, що шахрайство шкодить не лише фінансовому стану, а й репутації та бренду організації [3].

PwC визначає шахрайство як умисний обман, спрямований на привласнення фінансових коштів, майна чи законних прав [9].

Поняття «шахрайство» закріплене в статті 190 Кримінального кодексу України, згідно з яким шахрайство - це незаконне заволодіння чужим майном або набуття права на нього через обман чи зловживання довірою [12].

У статті 222 Кримінального кодексу України визначено поняття шахрайства з фінансовими ресурсами як «надання свідомо неправдивої інформації органам державної влади, органам влади АР Крим, місцевого самоврядування, банкам або іншим кредиторам з метою отримання субсидій, субвенцій, дотацій, кредитів чи податкових пільг» [12]. Цей злочин передбачає використання неправдивих даних з метою отримання фінансових чи податкових переваг, таких як субсидії, дотації чи кредити. Особливістю такого правопорушення є наявність умислу, оскільки правопорушник свідомо надає недостовірну інформацію, маючи на меті отримання матеріальних вигод.

Стосовно фінансового шахрайства, С. Чернявський визначає його як сукупність взаємопов'язаних суспільно небезпечних дій, спрямованих на привласнення чужого майна або отримання права на нього через обман чи зловживання довірою. Такі дії відбуваються у сфері правовідносин, що регулюються нормами фінансового права, і стосуються формування, розподілу, перерозподілу та використання фінансових ресурсів держави, суб'єктів господарювання і фізичних осіб [41].

Попри численні попередження з боку засобів масової інформації та інших джерел про різні шахрайські схеми, а також, як не дивно, навіть негативний особистий досвід, багато людей продовжують інвестувати кошти у сумнівні проєкти. На думку експертів, головною причиною цього є незмінне прагнення людей до легкого заробітку, яке навряд чи зникне в майбутньому

[29]. Це явище великою мірою базується на людській жадібності, яка стає основою для виникнення фінансових афер і шахрайств.

Крім того, фахівці звертають увагу на так званий "феномен довіри" [35]. В умовах загальної недовіри до держави та фінансових установ, люди, за своєю природою, схильні виявляти довіру до інших, часто без особливого упередження. Ця природна схильність, яка є важливою складовою людських взаємин у повсякденному житті та бізнесі, водночас стає вразливим місцем. Саме на цьому чиннику шахраї будують свої маніпуляції, використовуючи довіру людей у своїх корисливих цілях [29].

Таким чином, можна зробити висновок, що ключовими факторами, які сприяють поширенню шахрайства, є довірливість людей, бажання швидкого збагачення, низький рівень фінансової грамотності, а також небажання вивчати й розуміти основи фінансових питань.

Розвитку шахрайських схем у сучасному світі сприяють численні економічні фактори. Серед них - різноманітність фінансових інструментів, таких як різні форми грошей, цінні папери та фінансові послуги; значне збільшення кількості фінансових операцій; а також відкриття кордонів для вільного руху капіталу, товарів і послуг у контексті глобалізації. Це, своєю чергою, створює сприятливе середовище для зростання транснаціональної фінансової злочинності. У таких умовах довірливі інвестори, прагнучи зберегти або примножити свої кошти, часто стають жертвами шахрайських схем [10].

Зазвичай шахрайство, пов'язане з незаконним привласненням фінансових ресурсів, здійснюється групами осіб або організованими злочинними структурами, які мають широкі зв'язки не лише в Україні, а й за її межами. Організаторами та виконавцями таких злочинів часто виступають люди з високим рівнем економічних знань і значним практичним досвідом, які володіють розгалуженими контактами в органах державної влади. Так звані "білокомірцеві" злочинці здійснюють свої дії без застосування насильства, використовуючи обман або маніпуляцію інформацією для отримання

фінансової вигоди. Як зазначають дослідники, ці особи, як правило, належать до підприємницького середовища, є спеціалістами середнього або високого рівня у сфері фінансів, добре розбираються у законодавстві, зокрема податковому та банківському, і мають знання в бухгалтерському обліку. Часто вони також мають досвід роботи на державних посадах. Через це виявлення і боротьба з такими шахрайськими схемами нерідко стикаються зі значним спротивом з боку зацікавлених осіб та установ [16].

На сьогодні фінансове шахрайство стало досить поширеним явищем, яке зачіпає як бізнес, так і окремих громадян. В умовах складної економічної ситуації спостерігається значне зростання активності шахраїв. Таким чином, необхідно оновити напрямки державної фінансової політики, орієнтовані на подолання цього негативного явища.

1.2. Ідентифікація та мінімізація ризиків фінансового шахрайства

Фінансове шахрайство може зачіпати як державні, так і приватні фінанси. Під його вплив потрапляють фізичні та юридичні особи, а також держава, які під час своєї діяльності стикаються з низкою ризиків, що можуть прямо або опосередковано впливати на досягнення фінансових результатів.

У зв'язку з цим зростає важливість здатності ідентифікувати та мінімізувати потенційні ризики. Управління ризиками допомагає приймати обґрунтовані управлінські рішення, враховуючи чинники невизначеності та ймовірність виникнення непередбачуваних подій. Це дозволяє оцінити вплив таких подій на досягнення поставлених цілей.

Фінансове шахрайство має багато форм і методів, які постійно оновлюються та вдосконалюються. Через це виникають труднощі з їх систематизацією за чіткими ознаками чи критеріями. Однак, аналізуючи наявні класифікації та узагальнюючи основні характеристики фінансового шахрайства, можна виділити ключові його види (табл. 1.1).

Таблиця 1.1

Класифікація фінансового шахрайства щодо об'єкта шахрайських дій

Типи фінансового шахрайства, спрямовані на фізичних осіб	Типи фінансового шахрайства, спрямовані на юридичних осіб	Типи фінансового шахрайства, спрямовані на державу
Шахрайство з платіжними картками: незаконне отримання доступу до чужих коштів через злом пін-коду або використання інших шахрайських методів.	Фінансові махінації, що стосуються ресурсів юридичних осіб (внутрішні): підробка фінансової звітності.	Шахрайство, пов'язане з доходами держави.
Мобільне шахрайство: обман через телефонні дзвінки чи SMS, які мають на меті отримати дані банківської картки під вигаданими приводами.	Незаконне присвоєння активів, зокрема навмисне доведення до банкрутства.	Шахрайство у сфері витрат держави: використання бюджетних коштів не за призначенням; махінації в процесі державних закупівель.
Інтернет-шахрайство: обман через електронні листи, які видають за повідомлення від банків, з метою збору конфіденційної інформації.	Фінансові махінації, що стосуються ресурсів юридичних осіб (зовнішні): корупція та хабарництво; фіктивна підприємницька діяльність.	Шахрайство, що стосується ресурсів державних цільових фондів.
Фінансова піраміда: форма шахрайства, коли виплати попереднім учасникам здійснюються за рахунок внесків нових інвесторів.	Махінації у сфері управління персоналом; цінові спекуляції.	Шахрайство з активами державних підприємств, включаючи незаконне привласнення майна, корупційні дії та отримання хабарів.

Джерело: складено за даними джерела [2]

Фінансові махінації, спрямовані на фізичних осіб, мають на меті обманним шляхом заволодіти їхніми особистими даними, здійснити шахрайські дії через інтернет або використовувати схеми з «попередньою оплатою». Одним із прикладів такого шахрайства є фінансова піраміда, яка приваблює інвесторів обіцянками високого прибутку, але не надає реального продукту чи послуги. Виплати учасникам у таких схемах відбуваються за рахунок внесків нових вкладників.

Швидкий прогрес цифрових технологій і автоматизація фінансових операцій значно полегшують проведення розрахунків, але одночасно створюють нові ризики, пов'язані з онлайн-шахрайством [49]. Заволодіння персональними даними, паролями або доступом до інтернет-банкінгу може призвести до втрати заощаджень, використання шахраями кредитних лімітів або навіть оформлення нових позик від імені постраждалого. Це також несе загрози для фінансових установ, оскільки збільшується ймовірність зростання частки проблемних кредитів, виданих шахраям [6].

Фінансове шахрайство, що стосується підприємств, може проявлятися як у внутрішній, так і у зовнішній формі.

Внутрішнє шахрайство виникає, коли керівники або співробітники компанії здійснюють протиправні дії проти власної організації. Це може включати розкрадання активів, підробку фінансової звітності, ухилення від сплати податків, або надання недостовірної чи неповної інформації акціонерам і інвесторам. У такій ситуації підприємство може зіткнутися зі складнощами у фінансовому управлінні як у найближчій перспективі, так і в довгостроковому плані [7].

Зовнішнє шахрайство охоплює дії, спрямовані на обман підприємства зовнішніми контрагентами. Це можуть бути постачальники, які перебільшують витрати або завищують обсяги виконаних робіт. Клієнти також можуть бути причетними до шахрайських дій, наприклад, через несплату за послуги чи використання фальшивих купюр.

Фінансове шахрайство стосовно держави можна трактувати як сукупність економічних взаємозв'язків між державою та юридичними або фізичними особами під час формування, розподілу та використання державних фінансових ресурсів, що здійснюються через обман або зловживання довірою чи службовим становищем з метою отримання неправомірної вигоди [2].

Процес виявлення та зниження ризиків фінансового шахрайства може бути реалізований через різноманітні підходи, що враховують потреби та умови як зовнішнього, так і внутрішнього середовища. Ризик фінансового шахрайства можна охарактеризувати як ймовірність його виникнення та наслідки, що впливають на фінансову стабільність фізичних осіб, юридичних установ чи держави. Основним етапом у процесі управління ризиками є їхня ідентифікація, що включає визначення основних видів ризиків, які притаманні діяльності конкретного суб'єкта і можуть вплинути на його фінансовий стан або стратегію. Ідентифікація передбачає визначення ризиків у контексті їх взаємозв'язку з іншими факторами або джерелами, що можуть посилювати чи зменшувати ймовірність їх реалізації. Головною метою ідентифікації є виявлення, оцінка та опис ризиків, які можуть як сприяти, так і перешкоджати досягненню поставлених цілей суб'єкта.

Заходи та методи виявлення й зменшення ризиків фінансового шахрайства мають охоплювати такі ключові аспекти:

- визнання наявності проблеми та оцінка її потенційної загрози;
- дослідження сучасних шахрайських схем, їхніх особливостей і напрямків;
- виявлення критичних слабких місць у системі управління фінансовими ресурсами, найбільш уразливих до шахрайства;
- аналіз підходів до управління ризиками фінансового шахрайства;
- підвищення рівня фінансової грамотності;
- гнучкість та вдосконалення системи фінансового контролю;

- активізація співпраці з експертами у сфері фінансів та правоохоронними органами.

Основні способи запобігання фінансовому шахрайству зображені у таблиці 1.2.

Таблиця 1.2

Способи запобігання фінансовому шахрайству

Фізичною особою	Юридичною особою	Державою
ніколи не ділитися даними платіжних карток з іншими особами	встановити ефективну комунікацію з працівниками щодо попередження ризиків шахрайства	забезпечувати контроль за цільовим і раціональним використанням коштів державного та місцевих бюджетів
уникати відповіді на підозрілі повідомлення та не переходити за сумнівними лінками	розробити систему, яка забезпечує належну підготовку та перевірку фінансових звітів	протидіяти ухиленню від сплати податків і зборів.
завжди зберігати конфіденційність одноразових паролів	розподіляти обов'язки, повноваження та напрямки внутрішнього контролю	перевіряти законність, обґрунтованість та ефективність управління державними майновими правами
пройти ідентифікацію через свого оператора мобільного зв'язку	сприяти розвитку корпоративної культури	здійснювати нагляд за використанням державних резервів і запасів
підвищувати рівень фінансової обізнаності	створювати та публікувати зрозумілу та відкриту програму боротьби з фінансовим шахрайством в організації	моніторити цільове використання та своєчасне повернення кредитів і позик, отриманих під державні чи місцеві гарантії
тісно співпрацювати з правоохоронними органами	розробляти власну стратегію для отримання інформації про можливі шахрайства	сприяти прозорості та відкритості фінансових операцій
брати участь в навчальних та інформаційних заходах щодо боротьби з фінансовим шахрайством і покращення фінансової грамотності	створювати прозору політику санкцій щодо осіб, які здійснюють шахрайські дії	налагоджувати активну взаємодію з урядами інших країн і міжнародними організаціями у сфері боротьби з фінансовим шахрайством

Джерело: складено за даними джерела [2]

Кількість шахрайських схем значно зростає під час економічних криз та потрясінь. Нестабільна фінансова ситуація в країні може призводити до банкрутства фінансових установ, закриття підприємств, зменшення кількості робочих місць, втрати довіри до фінансово-кредитних інститутів та обмеження можливостей для отримання прибутку звичними способами. У таких умовах хаосу та невизначеності навіть сумнівні ініціативи, що обіцяють швидкий успіх, виглядають як можливість вирішити проблеми. Це штовхає людей до необдуманих і ризикованих дій для отримання прибутку. Мотиви таких дій можуть включати фінансові труднощі, схильність до ризику чи азарту, зовнішній тиск з боку інших осіб, а також відсутність суворого контролю. Найважливішим стимулом для шахраїв є можливість отримати надприбутки.

Фінансове шахрайство порушує економічні відносини, зокрема процеси формування, розподілу та використання фінансових ресурсів. Воно завдає значних збитків національній економіці, створює загрози для інвестиційної та підприємницької діяльності, а також негативно впливає на рівень доходів і добробут громадян. Саме тому, постійний пошук нових методів і вдосконалення існуючих підходів до протидії фінансовим зловживанням є вкрай важливим. Це зумовлено тим, що разом із розвитком методів боротьби зі шахрайством шахраї винаходять дедалі складніші схеми для обходу заходів контролю та запобігання.

1.3. Державне регулювання протидії фінансовому шахрайству

У процесі розвитку правової держави в Україні, впровадження демократичних перетворень та посилення принципу верховенства права у всіх сферах державного управління значення права невідно зростає. Порушення у фінансовому та банківському секторах створюють серйозну загрозу економічним інтересам суспільства. Завдані збитки громадянам, підприємствам і державі не лише підривають фінансову систему, а й

посилюють соціальну нерівність та погіршують міжнародну репутацію країни. Особлива небезпека фінансових і кредитних правопорушень полягає в тому, що вони сприяють розвитку інших злочинів.

За останнє десятиліття цифрові технології розвиваються стрімкими темпами, формуючи базу для впровадження інновацій в усі аспекти сучасного життя. Мобільні платежі, інтернет-банкінг, блокчейн, віртуальні активи, біометричні технології та інші рішення вже стали невід’ємною його частиною. Реалізація фінансових технологій (фінтех) у різних країнах залежить від особливостей законодавчого регулювання, рівня економічного розвитку, культурних відмінностей і потреб суспільства.

В Україні у 2020–2022 роках відбулося суттєве оновлення законодавства, пов’язаного з використанням фінансових технологій. У цей період було ухвалено низку ключових нормативно-правових актів. Зокрема, Україна адаптувала до національного законодавства основний регуляторний документ Європейського Союзу у сфері фінтеху – Директиву ЄС 2015/2366 «Про платіжні послуги на внутрішньому ринку» (PSD2). На основі цієї директиви був прийнятий Закон України «Про платіжні послуги» № 1591 від 30 червня 2021 року, який забезпечив розвиток інновацій на платіжному ринку та створив сучасне й безпечне правове середовище для фінтех-компаній в Україні.

Важливим кроком на шляху інтеграції України з Європейським Союзом у сфері цифрових послуг стало ухвалення Закону України «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII від 5 жовтня 2017 року. Цей закон встановив правові та організаційні основи для електронної ідентифікації та надання довірчих електронних послуг. У ньому визначено права й обов’язки учасників правовідносин у цих сферах, а також механізми державного контролю за дотриманням законодавчих вимог. Окрім того, Закон України «Про захист персональних даних» № 2297-VI від 1 червня 2010 року, хоча й не є вузькоспеціалізованим для фінансових технологій, відіграє важливу роль у будь-якій сфері, де здійснюється обробка персональних даних.

У фінансових технологіях захист таких даних є ключовим елементом для забезпечення довіри користувачів і дотримання міжнародних стандартів [33].

Національний банк України впровадив вимогу до постачальників платіжних послуг використовувати посилену автентифікацію користувачів для зниження ризиків шахрайства. Це рішення спрямоване на виконання положень Закону України "Про платіжні послуги" та узгодження українського законодавства з нормами Європейського Союзу у сфері платіжних операцій.

Відповідно до нових правил, провайдери платіжних сервісів зобов'язані впроваджувати розширену автентифікацію у таких ситуаціях:

- у разі надання віддаленого доступу до рахунків;
- під час здійснення онлайн-платіжних транзакцій;
- якщо є підозра на шахрайство чи інші незаконні дії, або за наявності відповідного ризику.

У підсумку цієї процедури формується унікальний код автентифікації, що прив'язує певну транзакцію до її суми та отримувача. Платіжні провайдери зобов'язані щоразу приймати цей код, коли користувач входить до свого рахунку або проводить віддалену фінансову операцію.

Отже, якщо раніше для здійснення онлайн-платежів було достатньо ввести реквізити картки та одноразовий пароль, тепер необхідно використовувати мінімум два рівні захисту. Це забезпечує впевненість у тому, що операцію проводить справжній власник платіжного засобу, а не злоумисник.

НБУ надав платіжним установам повну автономію у виборі технологічних рішень для впровадження посиленої автентифікації. Водночас регулятор встановив додаткові вимоги, спрямовані на підвищення безпеки фінансових операцій:

- провайдери платіжних сервісів повинні запровадити заходи та інструменти для виявлення незаконних або підозрілих транзакцій, враховуючи численні ризикові фактори, такі як списки скомпрометованих елементів

автентифікації, поширені схеми шахрайства та ознаки зараження шкідливим програмним забезпеченням;

- підвищено вимоги до безпеки операцій, включно з динамічним зв'язком між платіжною інформацією та кодом автентифікації;

- встановлено вимоги до захисту елементів посиленої автентифікації, програмного забезпечення та засобів для віддаленого зв'язку, які залучені до їх обробки;

- визначено вимоги до незалежності елементів посиленої автентифікації, що запобігає їх компрометації;

- окремо зазначено ситуації, коли постачальники платіжних послуг мають право не вимагати використання посиленої автентифікації;

- встановлено норми для забезпечення захисту конфіденційності та цілісності персональних даних користувачів;

- окреслено вимоги до електронного обміну даними між учасниками платіжного процесу та заходів безпеки, що гарантують цю взаємодію.

Ці норми зафіксовані в постанові Правління НБУ від 3 травня 2023 року № 58. Постанова набрала чинності 10 травня 2023 року, за винятком вимог, що стосуються електронної взаємодії між учасниками платіжного ринку та відповідних заходів безпеки. Ці вимоги почнуть діяти з 1 серпня 2025 року, синхронно з уведенням у дію глави 4 розділу IV Закону України "Про платіжні послуги" [17].

В Україні ухвалено Національну стратегію розвитку фінансової грамотності до 2030 року (далі – Стратегія), яка спрямована на підвищення фінансової обізнаності громадян. Ініціатором розробки даного документа виступив НБУ. Сьогоднішні реалії ставлять перед нами низку викликів: прийняття фінансових рішень в умовах нестабільності, розмаїття складних фінансових інструментів, активний розвиток цифрових технологій та зростання випадків шахрайства. Для ефективного реагування на ці загрози необхідно об'єднати зусилля задля формування системи фінансової грамотності. Це допоможе не лише покращити рівень поінформованості, але й

фінансової інклюзії населення. У результаті системної роботи громадяни набудуть навичок управління особистими, сімейними та бізнес-фінансами навіть у складних умовах.

Впровадження Стратегії дозволить значно розширити заходи, спрямовані на розвиток фінансової грамотності, та охопити нові цільові групи. Якщо раніше основна увага приділялася дітям і молоді, то тепер акцент зміщено на підприємців, ветеранів, людей старшого віку та внутрішньо переміщених осіб. Реалізація Стратегії передбачає досягнення п'яти стратегічних цілей, спрямованих на формування фінансової стійкості та раціонального фінансового адміністрування серед українців:

Ціль 1. Повноцінна базова освіта у сфері фінансів. Для її реалізації передбачено низку ініціатив, спрямованих на підвищення фінансової грамотності дітей дошкільного віку, учнів та студентів. Зокрема, планується розробка сучасних навчальних матеріалів і вдосконалення освітніх програм. Важливою складовою цього процесу є створення об'єднання педагогів-експертів із фінансової грамотності, що сприятиме ефективному впровадженню нового обов'язкового шкільного предмета "Підприємництво та фінансова грамотність".

Ціль 2. Відповідальне фінансове життя. Мета полягає в підвищенні фінансової обізнаності дорослого населення. У межах реалізації цієї цілі розроблятимуться освітні ресурси, які допоможуть громадянам опановувати фінансові навички на різних життєвих етапах. Особливий акцент буде зроблено на управлінні особистими фінансами в складних умовах, розумінні фінансових продуктів, економічних процесів, а також на обізнаності щодо прав і обов'язків користувачів фінпослуг.

Ціль 3. Підприємці з високим рівнем фінансової обізнаності. В Україні вперше запроваджується комплексний підхід до розвитку фінансової грамотності бізнесу. У межах цієї мети передбачено розробку структури фінансових компетенцій для підприємців. Крім того, будуть організовані заходи, спрямовані на підвищення обізнаності власників малого бізнесу та

підприємців-початківців щодо фінансових сервісів та інструментів, які допоможуть їм успішно розвивати свою справу.

Ціль 4. Розвиток знань у сфері цифрових фінансів. Стратегія приділяє значну увагу цифровій фінансовій грамотності, оскільки воєнні реалії показали українцям важливість безперешкодного доступу до фінансових сервісів онлайн та навичок їх використання. У рамках досягнення цієї мети передбачено розробку освітніх ресурсів і проведення заходів, спрямованих на підвищення обізнаності щодо цифрових фінансових сервісів, кібербезпеки та захисту платежів. Окремий акцент буде зроблено на використанні інтерактивних цифрових рішень для покращення фінансових навичок.

Ціль 5. Створення ефективного середовища для фінансової освіти. Ця ціль спрямована на розвиток фінансово-освітньої екосистеми в Україні та зміцнення партнерства як усередині країни, так і на міжнародній арені. У рамках реалізації Стратегії планується регулярний моніторинг фінансової обізнаності різних цільових груп та проведення опитувань. На основі отриманих даних документ буде оновлюватися, враховуючи актуальні виклики та потреби. Для громадян розроблятимуться онлайн-інструменти, які дозволять самостійно оцінити свої знання та виявити прогалини у фінансових навичках. Одним із ключових завдань є робота з мотивацією населення та зміна ставлення до фінансових питань, що сприятиме формуванню відповідальної фінансової поведінки [19].

На даний момент спостерігається значне зростання фінансового шахрайства, яке з року в рік набуває все більшого поширення. Це явище має складну економічну природу, що спонукає людей шукати можливості для швидкого заробітку. Водночас варто зазначити, що поточне законодавство України має недоліки, що створює умови для шахраїв розробляти нові схеми обману, вважаючи, що їм вдасться уникнути покарання за свої вчинки. Тому першочерговим завданням є удосконалення державного регулювання у сфері боротьби із фінансовим шахрайством.

Висновки до розділу 1

У сучасному світі науковий та технічний прогрес призводить до того, що проблема шахрайства стає все більш актуальною. Хоча розвиток технологій покращує якість життя, він також сприяє поширенню негативних явищ, зокрема шахрайства, яке охоплює різні сфери суспільства. Зараз шахрайство стає все складнішим, оскільки злочинці поєднують передові технології з сучасними психологічними методами, що робить його ще більш небезпечним.

Фінансове шахрайство може впливати як на державні, так і на приватні фінанси. Під його дію потрапляють як фізичні, так і юридичні особи, а також сама держава, які в процесі своєї діяльності стикаються з різноманітними ризиками, що можуть безпосередньо чи опосередковано вплинути на досягнення бажаних фінансових результатів. У зв'язку з цим стає все важливішим вміння виявляти та зменшувати можливі ризики. Управління ризиками дозволяє приймати зважені управлінські рішення, враховуючи фактори невизначеності та ймовірність виникнення непередбачених ситуацій, що дає змогу оцінити їхній вплив на досягнення поставлених цілей.

У процесі формування правової держави в Україні, реалізації демократичних змін та зміцнення принципу верховенства права у всіх сферах державного управління роль права постійно зростає. Останні десятиліття цифрові технології розвиваються дуже швидко, створюючи основу для інновацій в усіх аспектах сучасного життя. Впровадження фінансових технологій в різних країнах залежить від особливостей законодавчого регулювання, рівня економічного розвитку, культурних особливостей і потреб суспільства. Останнім часом в Україні відбулося суттєве оновлення законодавства, що стосується використання фінансових технологій. Водночас варто зазначити, що сучасне законодавство України має певні недоліки, що дає можливість шахраям розробляти нові схеми обману, сподіваючись уникнути покарання. Тому важливим завданням є вдосконалення державного контролю в сфері боротьби з фінансовим шахрайством.

РОЗДІЛ 2

ОЦІНКА РЕЗУЛЬТАТИВНОСТІ ПРОТИДІЇ ФІНАНСОВОМУ ШАХРАЙСТВУ

2.1. Типові схеми виявлення фінансового шахрайства

На сьогодні фінансове шахрайство стало дуже поширеним і швидко розвивається. Сучасні шахраї застосовують різноманітні методи обману, від простих до більш складних маніпуляцій. З розвитком науково-технічного прогресу все менше людей здійснюють готівкові платежі, що збільшує значення банківських карток у фінансових операціях. Це, в свою чергу, сприяє поширенню фінансового шахрайства.

Однією з найпоширеніших схем фінансового шахрайства є встановлення шахрайських пристроїв на банкоматах для отримання готівки. До таких пасток належать приховані камери, накладні клавіатури та пристрої (скіммери), що крадуть особисту інформацію з банківських карток. Скіммери зазвичай встановлюються на картоприймач або всередину нього, зчитуючи дані картки. Це частіше трапляється з картками, що мають лише магнітну стрічку, оскільки безконтактні картки та картки з чіпом мають кращий захист [1].

Наступним кроком шахраї створюють копію картки фізичної особи для зняття готівки. Для цього їм також необхідно знати пін-код, який вони отримують за допомогою прихованої камери або накладки на клавіатуру, що записує натиснуті цифри.

Іншою поширеною схемою є SMS-шахрайство. Шахраї надсилають повідомлення на мобільні телефони з різним змістом. Таке SMS може містити інформацію, ніби від імені банку, про блокування картки і необхідність термінового дзвінка за вказаним номером. Або ж повідомляється, що з платіжної картки користувача було здійснено переказ коштів, і надається номер телефону для уточнень. Коли людина зателефонує, шахраї зможуть отримати одноразовий пароль, який надійде в іншому SMS. Заволодівши цією

інформацією, вони можуть отримати доступ до фінансових ресурсів на банківському рахунку потерпілого. Шахраї також можуть надсилати повідомлення нібито від імені друга чи родича, просячи позичити певну суму грошей. Для цього вони злочинним шляхом отримують доступ до акаунтів у соціальних мережах і звертаються до людини від імені її знайомих.

Ще однією схемою є телефонне шахрайство, яке є одним із найпоширеніших видів фінансових злочинів. Злочинці телефонують та намагаються переконати людину розкрити особисту, фінансову або конфіденційну інформацію чи переказати кошти. Їхня мета - отримати дані банківських карток, паролі, або коди з SMS-повідомлень, надісланих банками чи мобільними операторами. Типовими ознаками таких дзвінків є створення тривожної ситуації, психологічний тиск та нагнітання поспіху з боку співрозмовника.

Сценарії телефонного шахрайства можуть бути різноманітними. Наприклад, людині повідомляють про виграш великої суми грошей, але для її отримання вимагають переказати комісію на вказаний рахунок. Інший поширений варіант - шахрай представляється працівником служби безпеки банку, заявляючи про кібератаку на банківську систему. Він запевняє, що для захисту коштів необхідно тимчасово перевести їх на "резервний" рахунок. Ще одна схема стосується осіб, які продають товари через інтернет. Шахрай, видаючи себе за покупця, обіцяє здійснити оплату на банківську карту, але спершу вимагає інформацію про карту та одноразовий код підтвердження. Такі дзвінки часто роблять у години, коли людина перебуває у стані втоми - рано вранці, наприкінці робочого дня або тижня. У такі моменти уважність, пам'ять і здатність критично сприймати інформацію знижуються. Шахраї створюють нервову атмосферу, що сприяє збентеженню та помилкам з боку жертви [38].

Текстові шахрайства, як і телефонні, стають дедалі хитрішими, використовуючи цифрові канали для обману людей. Шахраї активно користуються швидкістю та зручністю текстових повідомлень, щоб змусити

жертв розголошувати особисті дані або брати участь у шахрайських схемах. Найпоширеніші форми текстових шахрайств включають:

- смішинг (SMS-фішинг): шахраї надсилають повідомлення, які маскуються під офіційні організації, наприклад банки чи державні установи, щоб змусити одержувачів перейти за небезпечними посиланнями чи поділитися конфіденційною інформацією;
- фармінг: цей метод схожий на фішинг, але полягає у перенаправленні користувачів на підроблені веб-сайти через текстові повідомлення, де вони можуть ненавмисно надати логін або фінансові дані;
- шахрайство з підписками: жертва отримує текст про нібито оформлену підписку на послугу, за яку зніматимуться гроші, якщо вона не скасує її. Це призводить до фінансових втрат;
- фейкові заклики до благодійності: шахраї грають на почуттях співчуття, розсилаючи прохання про пожертвування для вигаданих благодійних організацій, особливо під час кризових ситуацій.

Наступна схема полягає у викраденні фінансового номера телефону, що використовується для прив'язки до банківських рахунків. На цей номер надходять повідомлення з кодами підтвердження, паролями для доступу до банківських сервісів і даними про стан рахунків.

Шахраї спочатку двічі поповнюють телефон на невеликі суми, а потім здійснюють дзвінок і одразу завершують його. Маючи дані про останні суми поповнень і номер останнього вхідного виклику, вони звертаються до оператора мобільного зв'язку з проханням відновити SIM-карту як загублену. У результаті шахраї отримують контроль над фінансовим номером жертви. Це дає їм доступ до інтернет-банкінгу та одноразових паролів для підтвердження операцій.

Ще однією популярною схемою є шахрайство в сфері онлайн-покупок. Людина переказує гроші шахраям, але так і не отримує обіцяний товар. Існують кілька характерних ознак, які можуть викликати підозру перед покупкою. Серед них: значно занижена ціна товару, наполегливість у швидкій

оплаті, обмежена інформація про продукт, незнання продавцем деталей чи технічних характеристик товару, а також перенаправлення з торгового сайту в месенджери для подальшого спілкування.

У цифровому середовищі фішинг продовжує бути хитрою і постійною загрозою, що використовує маніпуляції для отримання конфіденційної інформації. На відміну від телефонних та текстових шахрайств, які базуються на прямому контакті, фішинг відбувається через електронні листи або повідомлення, які здаються надійними, але насправді призводять на шахрайські веб-сайти або схиляють до розкриття важливих даних. Основні ознаки фішингових атак включають:

- підроблені електронні листи: шахраї змінюють заголовки листів, щоб вони виглядали надійно, часто копіюючи стиль відомих організацій чи осіб, щоб викликати довіру;
- шахрайські посилання: фішингові листи містять приховані лінки, які при натисканні перенаправляють на підроблені сайти, що збирають логіни та паролі або встановлюють шкідливе програмне забезпечення;
- імітація довірених осіб: шахраї можуть видавати себе за знайомих людей або представників фінансових установ, створюючи відчуття терміновості, щоб спонукати до швидкої реакції;
- цілеспрямований фішинг: цей вид фішингу адаптує повідомлення до конкретних осіб або компаній, часто використовуючи їх особисті дані для збільшення шансів на успіх.

Інтерес до криптовалют сьогодні залишається значним. Водночас із цим виникає загроза шахрайств, які продовжують ставити під ризик недосвідчених інвесторів. Шахраї використовують привабливість цифрових валют, щоб реалізувати маніпулятивні схеми. Щоб уникнути цих небезпек, потрібно бути уважними, ретельно перевіряти інформацію та ухвалювати обґрунтовані рішення.

Найпоширеніші види криптовалютних шахрайств:

- фальшиві первинні пропозиції монет (ICO): шахраї запускать неіснуючі криптовалюти з обіцянками високого доходу, щоб заманити інвесторів;

- фішинг: використання підроблених веб-сайтів і електронних листів для обману користувачів з метою отримання доступу до їхніх криптовалютних гаманців або приватних ключів;

- фінансові піраміди: обіцянки гарантованих прибутків з використанням коштів нових інвесторів для виплат старим учасникам, що призведе до краху схеми;

- фальшиві біржі: створення підроблених платформ для обміну криптовалюти, щоб шахраї змусили користувачів передавати свої кошти.

- шкідливі гаманці та додатки: підроблені програми, що виглядають як легітимні криптовалютні інструменти, але насправді спрямовані на крадіжку коштів.

Серед найпоширеніших схем шахрайства з криптовалютами сьогодні варто виділити схему Ponzi, яка орієнтована на введення інвесторів в оману. Шахраї обіцяють високі прибутки, але насправді виплати здійснюються не за рахунок реальних інвестицій, а за кошти нових учасників. Ця схема приваблює інвесторів обіцянками великих доходів, що підкріплюються значними виплатами, які насправді забезпечуються за рахунок внесків нових жертв. Це створює ілюзію високої прибутковості, що спонукає більше людей вкладати кошти в цей проєкт. Окрім того, новим інвесторам пропонують залучати інших учасників за додаткову винагороду, що веде до стрімкого зростання кількості людей, які долучаються до схеми. Однак коли нових учасників стає недостатньо для виконання зобов'язань перед тими, хто вже вкладав кошти, схема руйнується, і люди втрачають частину або всі свої гроші.

Схема "Pump and Dump" передбачає маніпуляції з ціною криптовалюти, коли її штучно підвищують, а потім, після того як інші інвестори починають активно купувати, швидко продають свої активи. У результаті, люди, які купили криптовалюту за завищеними цінами, втрачають свої інвестиції,

оскільки вартість активів різко падає. Для реалізації такої схеми шахраї часто використовують соціальні мережі, що дозволяють штучно підвищити інтерес до криптовалюти. Як правило, це стосується цифрових валют з низькою капіталізацією [43].

Пошук легітимних варіантів працевлаштування може бути ускладнений через постійну загрозу шахрайств у сфері зайнятості, де шахраї використовують різні маніпулятивні методи, щоб скористатися бажаннями шукачів роботи. Однією з найбільш поширених форм шахрайства стане обман, пов'язаний з роботою на дому, оскільки зростає попит на віддалену працю.

Шахрайства, пов'язані з роботою на дому, часто включають:

- фальшиві вакансії: шахраї видають себе за надійних роботодавців і пропонують привабливі вакансії з обіцянкою високих доходів за мінімальні зусилля;
- оплата за обладнання: потенційних жертв можуть вимагати заплатити за так звані робочі інструменти або навчальні матеріали, але після цього обіцяної роботи не буде;
- фішинг для збору особистих даних: шахраї під виглядом стандартних процедур адаптації запитують конфіденційну інформацію, що ставить під загрозу особисті дані жертв;
- шахрайство з переплатою: жертвам можуть надіслати підроблені чеки або платежі, і шахраї вимагатимуть повернення частини суми, залишаючи жертву відповідальною за всю вартість;
- шахрайство з грошовими мулами: деякі шукачі роботи стають учасниками незаконних схем, коли допомагають злочинцям переказувати гроші в обхід законодавства [18].

У корпоративному секторі найбільш поширеними видами шахрайства є:

- компрометація корпоративної електронної пошти (BEC). Це одна з найбільш серйозних загроз для бізнесу, коли зловмисники отримують доступ до електронної пошти компанії й надсилають фальшиві повідомлення, які виглядають достовірно. Мета – отримати гроші або доступ до конфіденційних

даних. Така схема може спричинити фінансові збитки, втрату даних і погіршення репутації компанії;

- шахрайство з фінансовими операціями. Одним із поширених прийомів є маніпуляція платіжними транзакціями. Наприклад, зловмисники можуть видавати себе за партнерів або постачальників, щоб змусити змінити реквізити для платежів;

- кіберзагрози від програм-вимагачів та вірусів. Таке шкідливе програмне забезпечення здатне блокувати доступ до критично важливих даних і вимагати викуп за їх розблокування, завдаючи шкоди роботі компанії;

- методи соціальної інженерії. Зловмисники використовують психологічні прийоми для введення в оману співробітників, щоб отримати доступ до закритої інформації або спровокувати незаконні фінансові дії.

У сфері корпоративної кібербезпеки використовуються більш складні методи захисту, ніж у роздрібному сегменті, через велику кількість та складність бізнес-процесів.

Штучний інтелект (далі ШІ) сьогодні активно використовується як для захисту банківських систем, так і для реалізації шахрайських схем. Банки застосовують можливості ШІ для посилення безпеки та оперативного реагування на загрози, водночас шахраї використовують ті ж технології для розробки складніших і більш адресних атак.

Як банки застосовують ШІ:

- моніторинг і виявлення загроз у реальному часі. Технології ШІ аналізують великі обсяги даних, дозволяючи знаходити підозрілі дії або аномальну поведінку клієнтів. Завдяки цьому банки можуть швидко реагувати на можливі шахрайські операції, відстежуючи навіть незначні відхилення від звичної поведінки користувачів;

- автоматизація дій у разі інцидентів. Алгоритми ШІ здатні автоматично блокувати небезпечні транзакції або обмежувати доступ до акаунтів, тим самим мінімізуючи наслідки шахрайства. Це значно скорочує час між виявленням загрози та її нейтралізацією;

- захист від кіберзагроз. Штучний інтелект аналізує трафік у мережах, розпізнаючи потенційно небезпечні дії, такі як спроби атак на сервери або несанкціоноване втручання. Крім того, ШІ здатний прогнозувати майбутні загрози на основі попереднього досвіду та сучасних тенденцій;

- покращення клієнтського досвіду. За допомогою ШІ банки пропонують клієнтам рекомендації щодо безпеки їхніх акаунтів та фінансових операцій, що допомагає захищати особисті дані.

Як шахраї використовують ШІ:

- автоматизація злочинних дій. Завдяки штучному інтелекту створюються реалістичні фішингові повідомлення, а процес їх розсилки значно спрощується;

- розробка складного шкідливого програмного забезпечення. ШІ допомагає створювати програми, які здатні обходити стандартні методи захисту;

- пошук вразливостей у системах. Аналізуючи великі обсяги даних, шахраї можуть знаходити слабкі місця в банківських системах або в облікових записах користувачів;

- імітація поведінки клієнтів. Використовуючи ШІ, шахраї можуть створювати дії, які важко відрізнити від реальних, ускладнюючи виявлення обману;

- персоналізовані атаки. Завдяки аналізу інформації про жертву атаки стають більш точними і дієвими [36].

Протягом останніх років фінансовий сектор зазнав значного зростання кіберзагроз, що вимагало активного розвитку заходів безпеки. Для забезпечення захисту фінансових операцій компанії збільшили інвестиції у сучасні технології та інноваційні системи протидії фінансовому шахрайству. Крім того, спостерігається поглиблення співпраці між банківськими установами, правоохоронними органами та технологічними компаніями. Обмін даними і координація спільних дій дозволяють більш ефективно протистояти фінансовому шахрайству і оперативно реагувати на нові виклики.

2.2. Аналіз рівня поширення фінансового шахрайства та ефективності заходів щодо його протидії

Фінансові злочини становлять серйозну загрозу для держави, яка перебуває у стані війни. У цей період особливо важливо забезпечити економічну стабільність та зберегти довіру до фінансової системи країни.

Війна створює умови, що сприяють виникненню нестабільності, вразливості та соціального хаосу, які стають підґрунтям для зростання рівня злочинності. Увага державних органів та ресурсів часто спрямована на вирішення нагальних військових проблем, тоді як громадяни залишаються менш захищеними, а контроль за фінансовими потоками послаблюється.

Неповний нагляд за використанням міжнародної фінансової та гуманітарної допомоги, що надходить від партнерів, лише ускладнює ситуацію, сприяючи поширенню фінансових порушень.

Термін "фінансові злочини" охоплює широкий спектр протиправних дій, пов'язаних із фінансами. Сюди належать ухилення від сплати податків, відмивання коштів, отриманих злочинним шляхом, шахрайство, зловживання платіжними картками та електронними грошима. Окрім втрати довіри, фінансові злочини завдають шкоди економіці країни, зменшуючи надходження до державного бюджету, що є вкрай необхідним у складний воєнний час.

Отже, зусилля держави та правоохоронних органів у протидії фінансовим злочинам повинні бути максимально прозорими та результативними. Це не лише сприятиме зміцненню економіки країни, а й стимулюватиме міжнародних партнерів до подальшого надання фінансової та військової допомоги.

У 2023 році середня сума однієї незаконної операції досягла 3065 гривень, що на 865 гривень більше, ніж у 2022 році. У той же час, у порівнянні з 2019 роком, коли середній обсяг становив 2100 гривень, відбулося збільшення на 965 грн. (рис. 2.1).

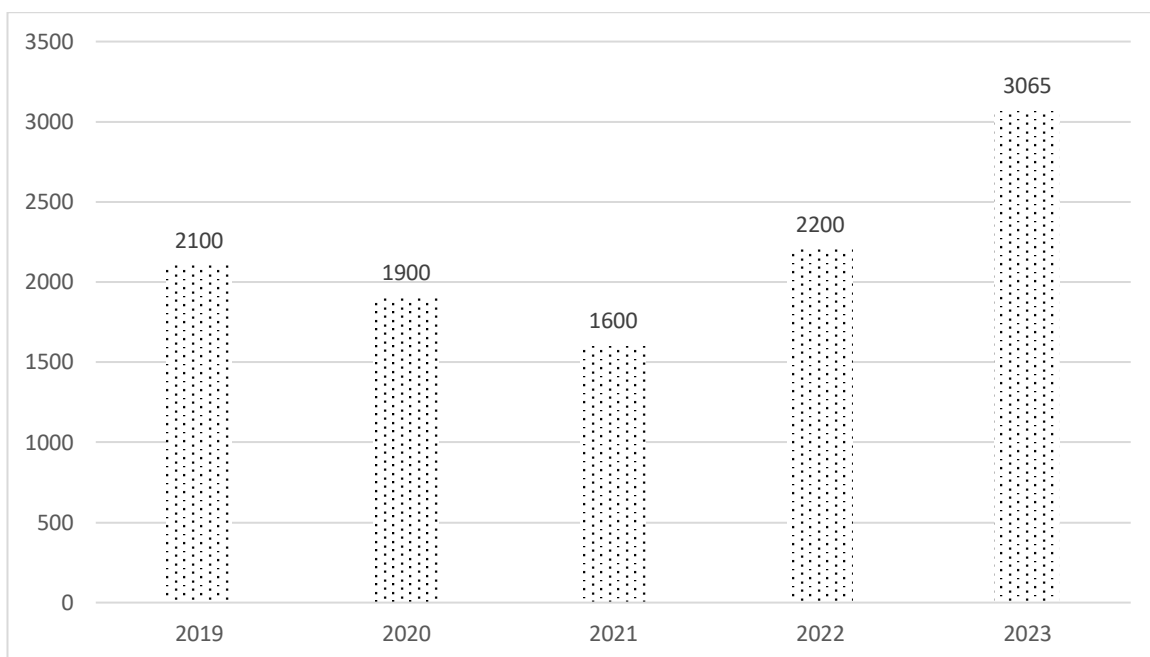


Рис.2.1. Динаміка середньої суми однієї незаконної операції за 2019-2023 рр., грн.

Джерело: складено за даними джерела [22]

У 2023 році кількість шахрайських операцій із платіжними картками, що призвели до фінансових втрат, збільшилася на 25% і досягла 272 тисяч. (рис.2.2).

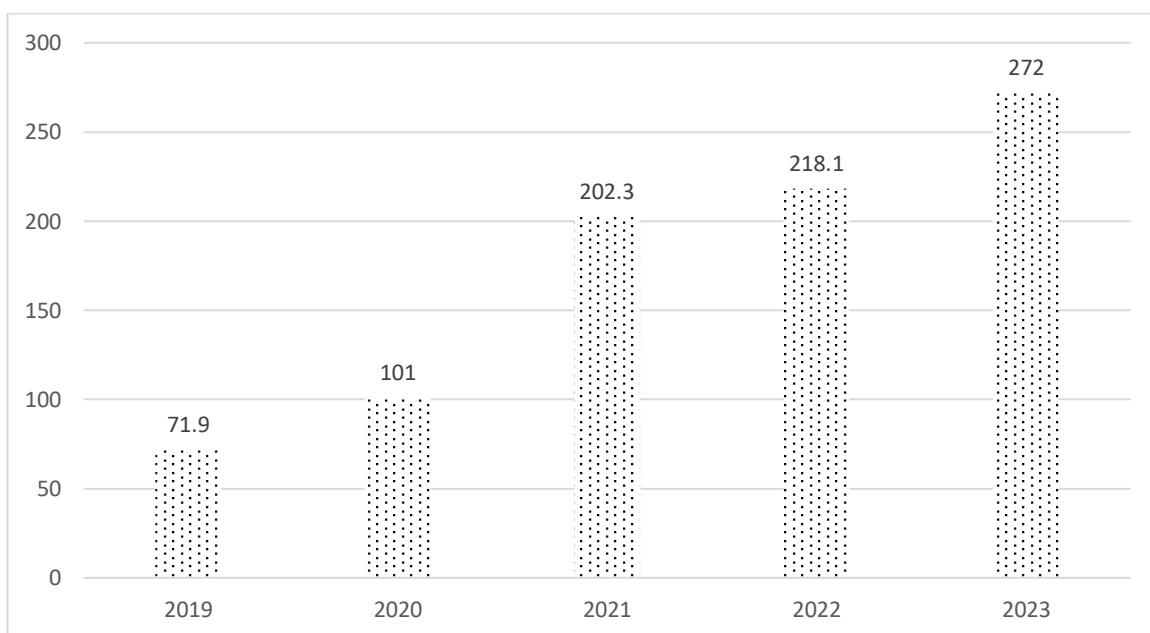


Рис.2.2. Динаміка кількості випадків шахрайства із банківськими картками за 2019-2023 рр., тис. операцій

Джерело: складено за даними джерела [22]

Згідно з даними НБУ, з 2023 року інформацію про втрати від шахрайських операцій надають не лише банки, але й небанківські фінансові установи та оператори поштового зв'язку. Проте їхній внесок у загальний обсяг збитків є незначним і становить лише 0,4%. Таким чином, основними жертвами шахрайських дій залишаються клієнти банків.

У 2023 році більшість випадків шахрайства були зафіксовані в Інтернеті - близько 83% усіх інцидентів, що трохи менше, ніж у 2022 році. Водночас частка злочинів, пов'язаних із використанням фізичних пристроїв, таких як POS-термінали та банкомати, зросла до 17%. Це можна пов'язати зі збільшенням кількості активних банківських карток на 13%, що сприяло росту операцій у торговельних точках і, відповідно, частішим випадкам шахрайства (рис.2.3).

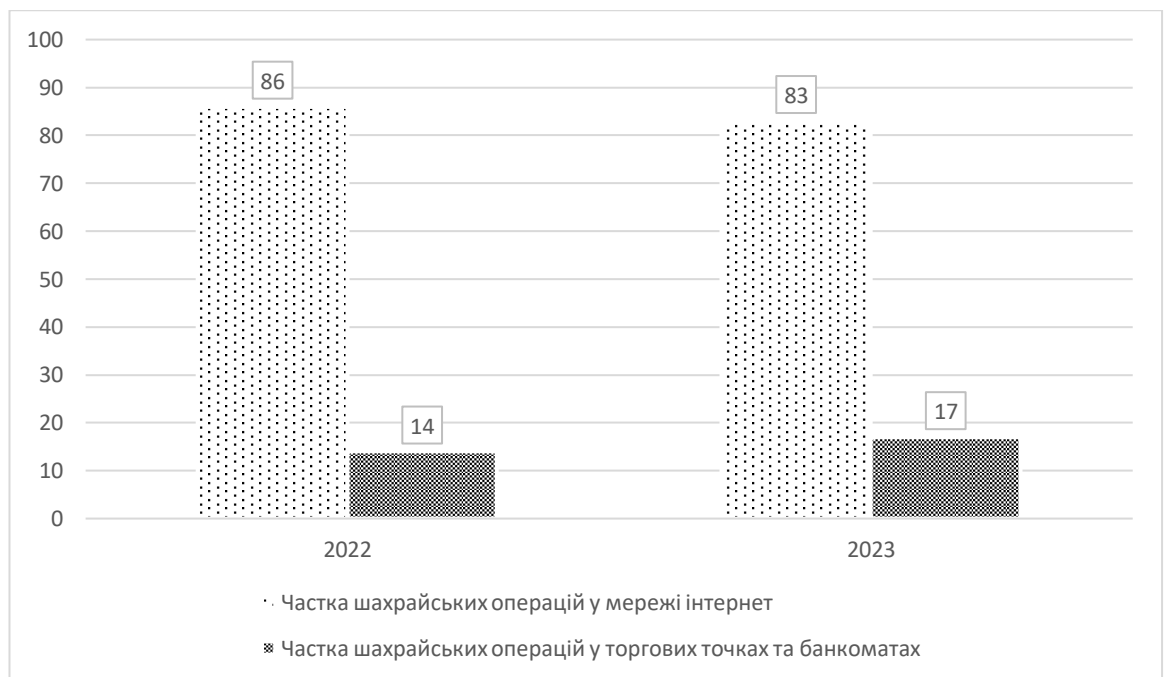


Рис.2.3. Частка шахрайських операцій у 2022-2023 рр., %

Джерело: складено за даними джерела [23; 24]

Основна частина шахрайських дій у 2023 році була пов'язана з тим, що клієнти самі розголошували свої особисті дані. На методи соціальної інженерії припало близько 80% загальної суми збитків. Порівняно з 2022 роком цей показник зріс більше ніж у півтора раза.

Під час повномасштабної війни в Україні спостерігається різке зростання кількості шахрайських злочинів. У 2023 році було відкрито 82 609 кримінальних проваджень за ст. 190 Кримінального кодексу України («Шахрайство»), що стало найвищим показником за останні роки. Кількість відкритих проваджень збільшилась у 2,6 раза у 2023 році порівняно з 2022 роком. Рекорд, що був зафіксований у 2013 році, складав 47 142 нових справ. У наступні роки ця кількість поступово зменшувалась, поки не розпочалося повномасштабне вторгнення. Окрім того, частка справ за ст. 190 ККУ, які потрапляють до суду, значно знизилась. У 2021 році цей показник становив 34%, а за останні два роки він знизився до 18% (рис.2.4).

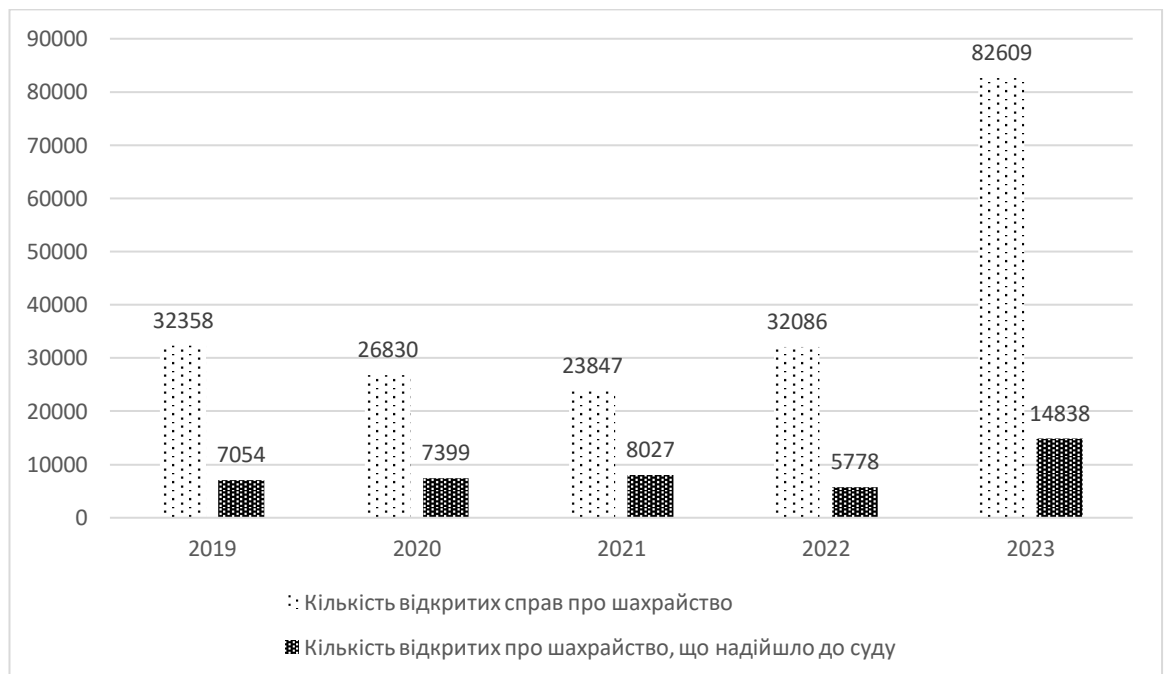


Рис.2.4. Динаміка кількості справ про шахрайство за 2019-2023 рр., од.

Джерело: складено за даними джерела [14]

В Україні існує низка шахрайських схем, що безпосередньо пов'язані з фінансовою діяльністю держави. Звернемо увагу на підсумки роботи Держаудитслужби та Держфінінспекції, а також їх регіональних підрозділів (рис. 2.5).

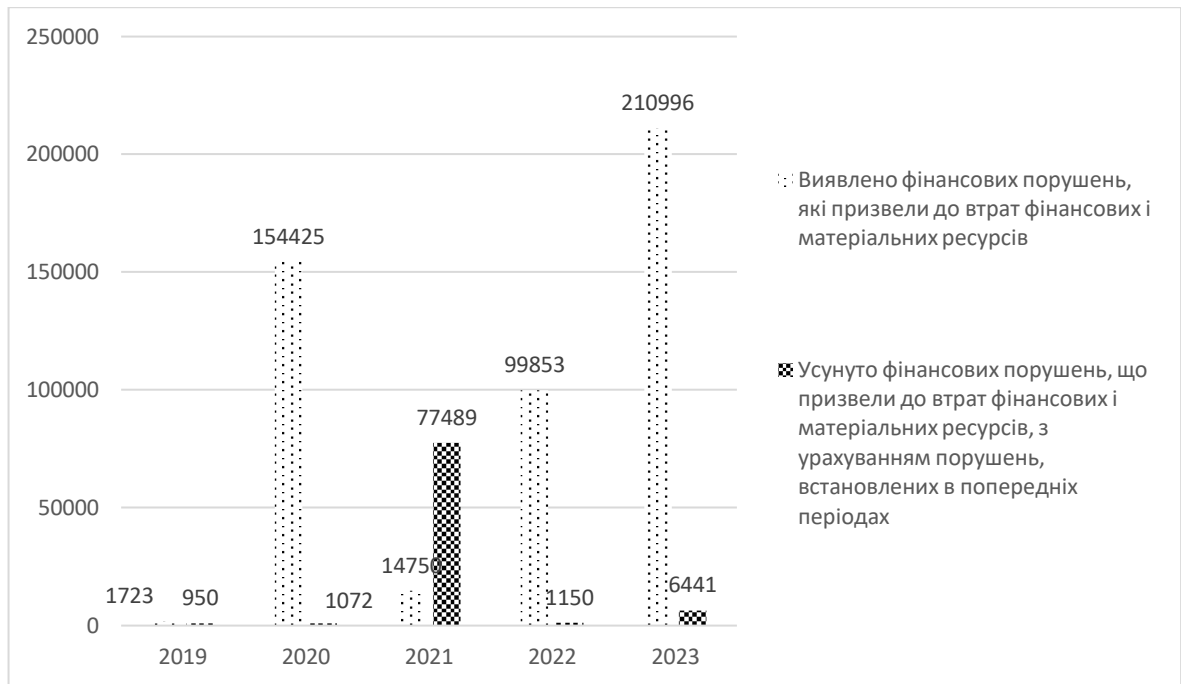


Рис.2.5. Динаміка виявлених та усунутих фінансових порушень, що спричинили втрати фінансових та матеріальних ресурсів у 2019-2023 роках, млн. грн.

Джерело: складено за даними джерела [5]

У 2023 році за підсумками проведених ревізій було зафіксовано фінансові та матеріальні порушення, що призвели до втрат на суму понад 210996 млн. грн. Як свідчить рис. 2.5, це найбільший обсяг таких втрат за аналізований період. Найбільша сума усунутих порушень була досягнута у 2021 році - 77 489 млн. грн.

Також варто звернути увагу на аналіз кількості вручення письмових повідомлень про підозру у кримінальних правопорушеннях та кількості осіб, які були притягнуті до адміністративної відповідальності (рис. 2.6). Протягом аналізованого періоду спостерігається наступна тенденція: кількість письмових повідомлень про підозру у вчиненні кримінальних правопорушень збільшилась на 41 випадок, а число осіб, притягнутих до адміністративної відповідальності, зменшилося на 1562 особи. Загалом це негативна тенденція, оскільки за аналізований період кількість осіб, притягнутих до адміністративної відповідальності скоротилась майже на 70%.

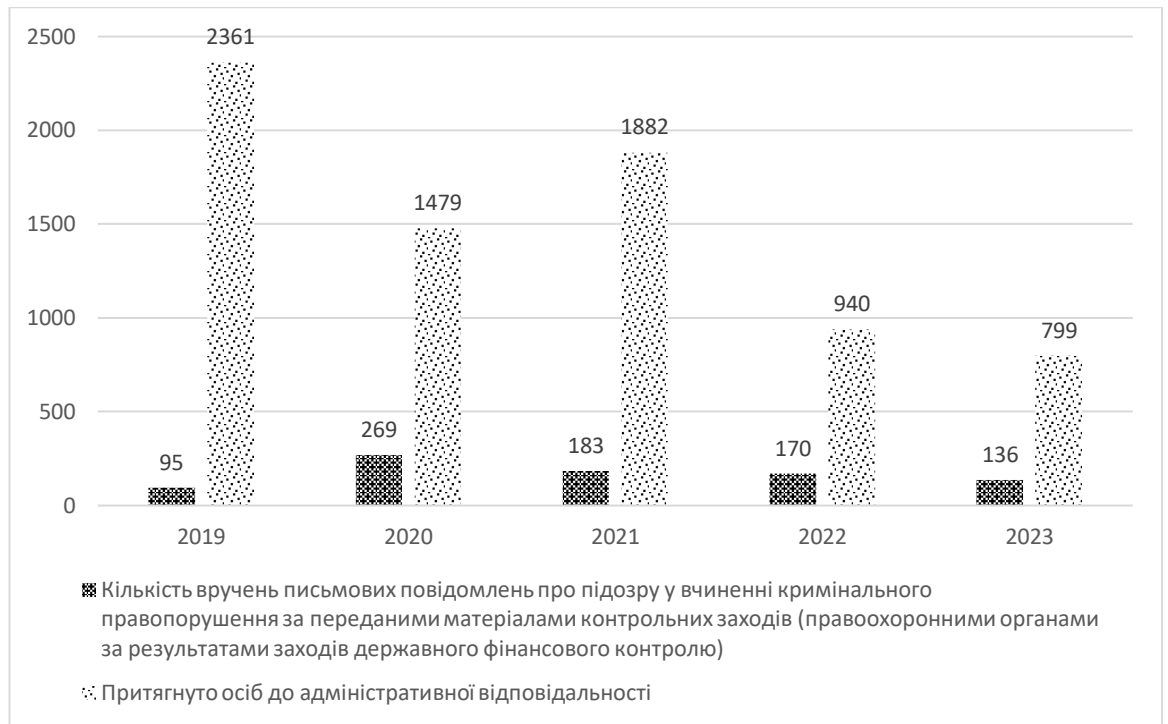


Рис.2.6. Динаміка вручень письмових повідомлень про підозру у кримінальних правопорушеннях та осіб, притягнутих до адміністративної відповідальності, у період 2019-2023 років, од.

Джерело: складено за даними джерела [5]

Ситуація в країні залишається складною, оскільки зростає як кількість шахрайських схем, так і масштаби недоотриманих фінансових та матеріальних ресурсів. Незважаючи на те, що виявлення таких порушень є результатом проведених ревізій і контролю, кількість письмових повідомлень про підозру залишається недостатньою. Ще менше випадків, коли винні особи реально несуть відповідальність за свої дії. Це зумовлено значною латентністю шахрайських дій, які часто виявляються лише з часом, створюючи серйозні ризики для підприємств і громадян.

Шахрайські операції демонструють зростання у всьому світі. За даними Statista, у 2022 році обсяг таких транзакцій збільшився на 3,4%, досягнувши \$33,45 млрд. У 2023 році, за попередніми оцінками, сума шахрайства з використанням банківських карток зросла до \$36 млрд, і це без урахування даних із США (рис.2.7). Експерти зазначають, що кожна третя або четверта

шахрайська операція відбувається саме в США. Враховуючи це, загальний обсяг шахрайства у світі, ймовірно, перевищує \$40 млрд.

Рік за роком кількість незаконних операцій збільшується разом із поширенням фінансових сервісів у різні сфери життя та зростанням популярності онлайн-шопінгу.

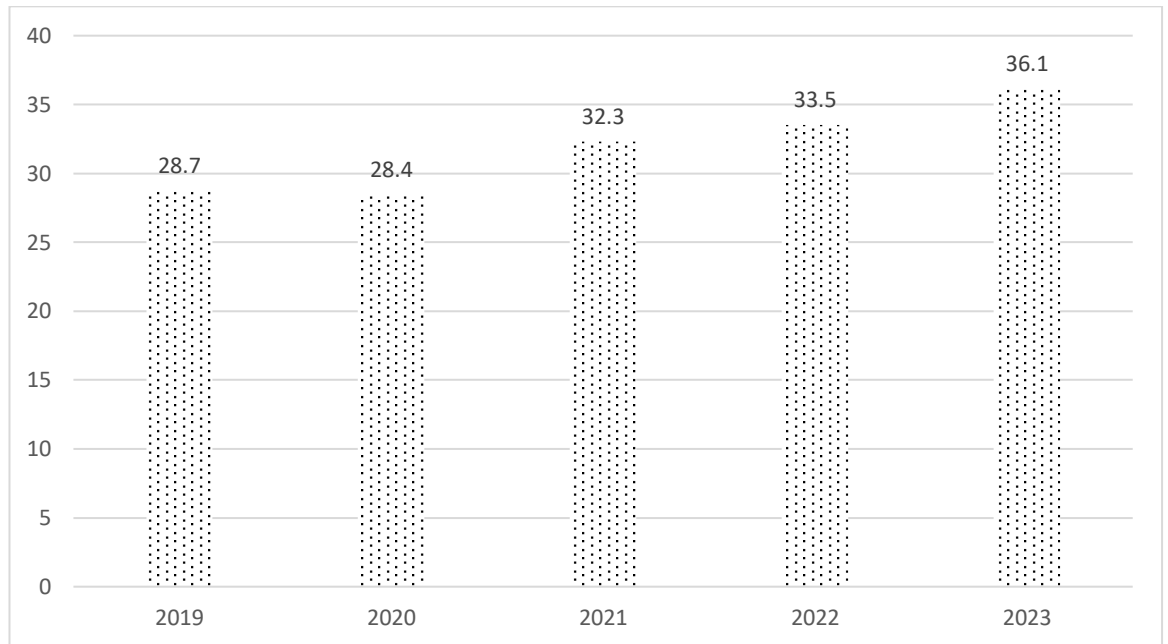


Рис.2.7. Динаміка обсягу шахрайських операцій із банківськими картками у світі у 2019-2023 рр., млрд. дол. США

Джерело: складено за даними джерела [45]

Середній розмір збитків від шахрайства залишається відносно невеликим. Згідно з даними консалтингової компанії Merchant Cost Consulting, близько 33% усіх втрат припадає на операції вартістю до \$50. Транзакції у діапазоні від \$50 до \$99 становлять 22% загального обсягу збитків, а шахрайські дії на суми від \$100 до \$299 складають 24% від загальної кількості випадків. Як і в Україні, у багатьох інших країнах власники банківських карток не завжди дбають про безпеку своїх фінансів. Тільки 59% користувачів активують сповіщення про шахрайські дії та транзакції. До того ж, 22% власників карток зовсім не переглядають виписки за своїми рахунками, що значно ускладнює виявлення можливих випадків шахрайства [45].

Одним із найбільш поширених видів фінансових злочинів є шахрайство. Тому діяльність правоохоронних органів має охоплювати не лише

розслідування та покарання винних, але й упровадження превентивних заходів, які допоможуть запобігти таким правопорушенням у майбутньому.

Висновки до розділу 2

Фінансове шахрайство становить серйозну загрозу для економічної стабільності країни та добробуту її громадян. Дослідження свідчать, що найбільш поширеними економічними злочинами є хабарництво, зловживання владними повноваженнями, корупція, кіберзлочини, махінації у сфері закупівель тощо.

Розвиток інформаційних технологій у фінансовому секторі сприяє появі нових форм злочинів. До найпоширеніших видів шахрайства належать: SMS-обман, телефонні афери, фішинг, смішинг, фармінг, шахрайство, пов'язане з підписками, підроблені заклики до благодійності, махінації з криптовалютами, кіберзагрози від вірусів та програм-вимагачів, а також використання штучного інтелекту для злочинних цілей.

На сьогодні фінансове шахрайство розглядається як серйозна загроза для суспільства. Варто зазначити, що кількість таких правопорушень помітно збільшилася, але процес їхнього виявлення, доведення та притягнення винних до відповідальності залишається надзвичайно складним. Як наслідок, у більшості випадків порушники закону уникають покарання.

Шахрайські фінансові операції демонструють тенденцію до зростання на глобальному рівні. За інформацією Statista, у 2022 році їхній обсяг зріс на 3,4%, досягнувши \$33,45 млрд. У 2023 році, за попередніми прогнозами, масштаби шахрайства з банківськими картками сягнули \$36 млрд. З кожним роком кількість незаконних транзакцій збільшується через розширення фінансових послуг у різні сфери повсякденного життя та зростання популярності інтернет-магазинів. Таким чином, фінансове шахрайство перестає бути лише локальною проблемою, стаючи однією з ключових загроз на світовій арені.

РОЗДІЛ 3

НАПРЯМИ ВДОСКОНАЛЕННЯ ЗАХОДІВ ПРОТИДІЇ ФІНАНСОВОМУ ШАХРАЙСТВУ В СУЧАСНИХ УМОВАХ

3.1. Міжнародний досвід у сфері боротьби з фінансовим шахрайством та перспективи його застосування в Україні

Сучасний фінансовий світ активно інтегрується з цифровими технологіями та інноваціями, адаптуючи бізнес і споживачів до зручного та швидкого обслуговування без зайвих зусиль. Проте розвиток цифрових технологій супроводжується зростанням випадків шахрайства, зокрема у фінансовій сфері. Фінансове шахрайство залишається актуальною проблемою навіть сьогодні, так само, як і понад століття тому. Наприклад, відома історія італійця Чарльза Понці, який організував одну з перших резонансних схем обману інвесторів [47].

Розвиток технологій, крім позитивних змін у суспільстві, призвів до зростання кількості зафіксованих випадків шахрайства та збільшення кількості схем, які використовуються у фінансовій сфері. Сучасне фінансове шахрайство суттєво відрізняється за масштабами поширення, рівнем організованості, завданими збитками та методами конспірації від традиційних способів незаконного заволодіння майном, які раніше фіксувалися правоохоронцями.

Відмінними рисами фінансового шахрайства є:

- завдання збитків переважно в кредитно-фінансовій сфері;
- використання різноманітних способів злочинної діяльності – від маніпуляцій із даними до складних схем фінансових махінацій.
- застосування сучасних технічних засобів і великої кількості документів (бухгалтерських, банківських, господарських тощо) для реалізації злочинів [20].

Фінансове шахрайство, як окремий вид обману, передбачає свідоме використання незаконних методів або прийомів для отримання фінансової вигоди. Найчастіше такі випадки виникають у ситуаціях, де контроль відсутній або є недостатньо ефективним.

Згідно зі щорічним Звітом про шахрайство за 2022 рік [46], опублікованим UK Finance, масштаби шахрайства в платіжній сфері Великої Британії залишаються значними. У 2022 році злочинці викрали понад 1,2 мільярда фунтів стерлінгів через санкціоновані та несанкціоновані шахрайські операції, що в середньому становить більше 2300 фунтів стерлінгів втрат кожну хвилину.

Шахраї стають дедалі винахідливішими та наполегливішими у своїх злочинних діях. За даними одного з останніх досліджень, 79% американців вважають, що не забезпечують належного захисту своєї особистої інформації в Інтернеті. У 2022 році шахрайство з кредитними картками зросло більш ніж на 70%, а загальні втрати американців через фінансові махінації досягли 56 мільярдів доларів [50].

Попри різні підходи до визначення фінансового шахрайства та його компонентів, у міжнародній практиці виділяються основні його типи:

- крадіжка персональних даних. Це один із поширених видів шахрайства, що включає незаконне використання особистої інформації, такої як ім'я, дата народження чи номер соціального страхування, для отримання доступу до фінансових рахунків або активів. Дані можуть бути викрадені через фішингові атаки, кібератаки, викрадення кореспонденції або навіть придбані на чорному ринку;

- шахрайство з передоплатою. Передбачає внесення авансового платежу за товар чи послугу, яка в результаті не надається. До цього виду також належать приховані платежі, як-от додаткові комісії. Серед поширених прикладів – шахрайські перевезення під виглядом евакуації або здача в оренду неіснуючого житла, коли після отримання передплати шахраї зникають;

- шахрайство з касовими та підробленими чеками. Це форма банківського шахрайства, яка використовує тривалі терміни перевірки касових чеків для обману. За даними, кількість випадків цього шахрайства зросла на 65% з 2015 року;

- фальшиві благодійні організації – створення підроблених благодійних структур для збору коштів, зазвичай через готівку, криптовалюту, подарункові картки або банківські перекази;

- шахрайство з кредитними картками – крадіжка карток, створення їх копій або введення даних на підроблених веб-сайтах;

- оволодіння фінансовими акаунтами – захоплення доступу до онлайн-банківських рахунків;

- схеми Понці та інші інвестиційні обмани, пов'язані з внесками у вигадані програми чи проєкти;

- шахрайство у малому бізнесі (крадіжки, зловживання тощо) – збитки від крадіжок та нецільового використання коштів працівниками [48];

- шахрайство з податковими відшкодуваннями та «фальшиві» податкові агенції. Одним із найпоширеніших видів є обман з поверненням податків, що включає викрадення особистих даних. Злочинці подають податкові декларації на ім'я іншої особи, вказуючи неправдиві доходи для отримання максимального відшкодування, яке потім забирає шахрай. У 2020 році IRS виявила 5,2 мільйона шахрайських декларацій [3].

Згідно з інформацією із США, Великобританії, Швейцарії та Сингапуру, шахрайство є одним із ключових злочинів, пов'язаних із підозрілими фінансовими операціями. У звіті США щодо ризиків відмивання коштів на 2024 рік зазначено, що шахрайство залишається основним джерелом незаконних доходів, які потребують відмивання. Шахрайські схеми, такі як інвестиційні махінації, романтичні афери та шахрайство з авансовими платежами, завдають шкоди як фінансовим установам, так і звичайним громадянам. Зростання використання штучного інтелекту та криптовалют ускладнює розслідування таких злочинів.

У 2024 році було оновлено методологію Basel AML Index, інструмента для глобального аналізу ризиків відмивання коштів (AML). Головною зміною стало додавання показників, пов'язаних із шахрайством, що пояснюється його зростаючою роллю як злочину, який часто передує процесам відмивання коштів. Таке рішення враховує серйозні соціальні та економічні наслідки шахрайства. Внесені зміни торкнуться також спеціалізованих версій індексу, таких як Expert Edition і Expert Edition Plus.

Ініціативи FATF, INTERPOL та Egmont Group підкреслюють зв'язок між шахрайством і іншими видами злочинності, зокрема торгівлею людьми та фінансуванням поширення зброї. У Basel AML Index інтегровано показники шахрайства з урахуванням їхніх обмежень, а дані отримуються з Global Organized Crime Index у двох категоріях: фінансові злочини (шахрайство, податкові ухилення, розтрата); кіберзлочини (хакерство, використання шкідливого ПЗ, шахрайство з криптовалютами).

Вагомість показників шахрайства встановлена на рівні 5% для фінансових злочинів і 2,5% для кіберзлочинів. Зі списку показників було виключено три застарілі індикатори: прозорість компаній (дані Світового банку); стандарти аудиту (дані Всесвітнього економічного форуму); інформація від Tax Justice Network буде перенесена до іншого розділу.

У 2022 році у Великій Британії збитки від несанкціонованих шахрайських операцій (викрадення особистих даних) за допомогою платіжних карток, онлайн-банкінгу та чеків досягли 726,9 мільйона фунтів стерлінгів [53].

Прийнятий у Великобританії у 2023 році Новий Закон про економічну злочинність та корпоративну прозорість вводить новий злочин - «неприйняття заходів щодо запобігання шахрайству», який вимагає від організацій впровадження ефективних механізмів для попередження шахрайських дій з боку їхніх працівників, агентів або дочірніх компаній. У разі невиконання цих вимог компанія може бути притягнута до відповідальності, навіть якщо керівництво не брало участі у шахрайських діях. Це встановлює нові

стандарти корпоративної відповідальності, що сприяють підвищенню прозорості та доброчесності у веденні бізнесу.

Закон охоплює різноманітні види шахрайства, зокрема: надання недостовірної інформації з метою отримання фінансових переваг; зловживання службовими повноваженнями, наприклад, для здобуття незаконної вигоди; підробка бухгалтерських записів та інших документів.

Крім цього, Закон зобов'язує організації адаптувати процедури запобігання шахрайству відповідно до особливостей своєї діяльності. Це означає, що підходи мають відрізнятися залежно від розмірів і типу компанії: великі міжнародні корпорації потребують одних методів, а невеликі локальні підприємства – інших. Для цього організації повинні оцінювати ризики з урахуванням таких чинників, як масштаби їхньої діяльності, специфіка бізнесу, рівень співпраці з посередниками та попередній досвід інцидентів. Пропорційний підхід гарантує ефективність заходів без зайвого адміністративного навантаження.

Документ наголошує, що основою запобігання шахрайству є формування культури етичності та прозорості в організації на всіх рівнях. Керівники мають особисто демонструвати нульову толерантність до шахрайства, впроваджуючи антикорупційні принципи у всі процеси управління. Серед ключових заходів виділяють створення безпечних каналів для повідомлення про порушення, регулярне навчання персоналу та сприяння відкритому обговоренню етичних питань. Системи запобігання шахрайству повинні бути гнучкими та регулярно оновлюватися. Організаціям слід враховувати зміни у бізнес-середовищі, включаючи нові законодавчі вимоги, технологічні інновації або ризики, пов'язані зі світовими економічними чи політичними подіями. Постійний моніторинг допомагає виявляти слабкі місця та своєчасно впроваджувати покращення.

Використання електронних систем для запобігання шахрайству та інструментів цифрового контролю в США є одним із ключових напрямів сучасної міжнародної політики в галузі електронної комерції. Цей досвід може

бути адаптований в Україні шляхом: створення єдиної інформаційної системи для профілактики шахрайства в електронній торгівлі, яка об'єднуватиме різні платформи, бази даних та інформаційні ресурси про шахрайські дії; реформування законодавства щодо кримінальної відповідальності за шахрайство в електронній комерції; впровадження передових електронних систем і технологій штучного інтелекту для боротьби з такими злочинами; розширення міжнародної співпраці та активного залучення громадськості до просвітницької діяльності, спрямованої на запобігання шахрайству в сфері електронної торгівлі [11].

Вивчаючи механізми боротьби з корупцією та організованою злочинністю, включаючи їх транснаціональні прояви, слід зазначити, що у світі діють антикорупційні закони з екстериторіальною юрисдикцією. Це означає, що їх дія поширюється за межі країн, де вони були ухвалені. Найвідомішими серед них є Закон США про корупцію за кордоном 1977 року та Закон Великобританії про боротьбу з хабарництвом 2010 року. У країнах ЄС також прийняті подібні антикорупційні закони, але їх міжнародне застосування поки не набуло значного поширення. Юридична сила вищезгаданих законів базується на значному впливі економік США та Великобританії у світі, що дозволяє ефективно притягувати до відповідальності компанії, залучені до корупційних дій, і мінімізує можливості уникнення покарання [8, с.129].

В Італії боротьба з корупцією та організованою злочинністю знаходиться під контролем Міністерства внутрішніх справ. За останнє десятиліття поліція значно посилила свою активність у цій сфері. Одним із показових прикладів є масштабні конфіскації, проведені правоохоронними органами на основі судових рішень. Зокрема, на Сицилії було вилучено майно мафії на суму €300 млн, включаючи акції компаній, 60 гектарів землі та 220 будівель. Загалом за останні роки італійські органи влади конфіскували близько 10 тисяч об'єктів нерухомості, пов'язаних із мафією. Зазвичай ці будівлі передають громадським або державним організаціям, які займаються

соціальною допомогою малозабезпеченим сім'ям. Італійське правосуддя також послідовно застосовує жорсткі покарання до учасників злочинних угруповань.

Під керівництвом правоохоронців Німеччини, поліція низки європейських країн спільно з Бразилією та Панамою провела масштабну операцію, у ході якої було викрито та затримано близько ста осіб, підозрюваних у контрабанді кокаїну, відмиванні коштів і податкових злочинах. Операція проводилася за участю агентів Євроюсту та Європолу [52]. Основною метою були лідери мафіозної організації «Ндрангета», яка вважається однією з найвпливовіших злочинних структур у світі. Затриманим інкримінують корупцію, відмивання грошей, наркаторгівлю, ухилення від сплати податків та шахрайство. Значна частина доходів «Ндрангети» в даний час надходить від незаконного обігу наркотиків.

Діяльність мафіозного угруповання «Ндрангета» вийшла за межі Європи і охопила США, Мексику та країни Латинської Америки. У цих регіонах, за інформацією правоохоронців, клан створив великий центр для відмивання коштів. «Ндрангета» бере свій початок у Калабрії, одній із найбідніших областей Італії, і включає близько 150 калабрійських сімей.

Щороку їхня злочинна діяльність, яка охоплює торгівлю наркотиками й зброєю, корупцію, шахрайство, розбої та незаконне привласнення державних коштів, приносить прибуток понад €50 мільярдів. Операції клану розповсюджуються не тільки на всю Італію, але й на США, Австралію, Канаду, Німеччину, Австрію, Нідерланди, Бельгію, Аргентину, Колумбію та Мексику. На сьогодні «Ндрангета» є одним із головних постачальників кокаїну в Європу [21].

У Нідерландах діє трирівнева система протидії організованим злочинності та корупції. Більшість випадків корупції вирішуються безпосередньо всередині державних установ, таких як пенітенціарні заклади, податкові органи, Міністерство оборони та інші. Для цього в структурах функціонують спеціальні відділи внутрішніх справ або служби безпеки.

Зазвичай порушників карають шляхом звільнення, зниження в посаді або накладанням штрафів за завдані збитки.

З огляду на тривалий процес адаптації українського законодавства до стандартів ЄС, варто звернути увагу на Угоду про асоціацію між Україною та Європейським Союзом. У рамках цієї угоди передбачена співпраця у боротьбі з організованою злочинністю, корупцією у державному та приватному секторах, а також заходи для їх запобігання. Така співпраця спрямована на розв'язання ключових проблем у цих сферах [15; 34].

Збитки від зловживань онлайн-платформами продовжують зростати, оскільки злочинці використовують ці ресурси для обману своїх жертв. Це включає інвестиційні шахрайства, які просуваються через пошукові системи та соціальні мережі, шахрайства з покупками, які рекламуються на соціальних мережах і сайтах аукціонів. Зловмисники також активно застосовують шахрайські телефонні дзвінки, СМС та електронні листи, а також створюють підроблені веб-сайти та публікації в соцмережах, щоб обманом змусити людей розкрити свої особисті дані та паролі.

У світі, що стає все більш цифровим і взаємопов'язаним, шахрайства постійно змінюються і еволюціонують. Зростання цифрових ініціатив у фінансових установах сприяло збільшенню онлайн-шахрайства та фінансових втрат. Бурхливий розвиток цифрових технологій створив нові канали для шахраїв, що призвело до найвищих рівнів збитків від фінансових злочинів. Більш того, нові технології спрощують вчинення шахрайств, що залучає ще більше злочинців.

Багатоканальна комерція покращує взаємодію з користувачами, але одночасно створює нові можливості для шахраїв через проблеми з кібербезпекою та відсутність єдиного підходу до ідентифікації користувачів у цифровому і фізичному середовищах [54].

Ринок криптовалют сьогодні активно розвивається та стає все більш привабливим для покупців і інвесторів. Однак через недосконалість регулювання та відсутність ефективних засобів захисту криптовалютні

платформи залишаються вразливими для шахраїв. Злочинці, у свою чергу, вкладають великі ресурси в новітні технології та процеси, часто працюючи за принципом бізнесу і зосереджуючись на тих методах, які гарантовано приносять прибуток.

Таким чином, боротьба з фінансовим шахрайством є актуальною проблемою по всьому світу, і, як показує практика, технологічний прогрес лише сприяє збільшенню збитків від шахрайських дій. Це ставить питання про необхідність розробки сучасних засобів захисту даних та підвищення рівня фінансової грамотності серед населення.

3.2. Вдосконалення державної політики у сфері протидії фінансовому шахрайству

Сучасна політична та соціально-економічна нестабільність створює сприятливі умови для поширення шахрайства в Україні. Водночас, попри серйозні негативні наслідки для суспільства та економіки, ця проблема залишається недостатньо дослідженою в фінансовій науці, головним чином через відсутність чітких законодавчих заборон на фінансові шахрайства. Важливо зазначити, що навіть ухвалення відповідних законодавчих актів або економічні реформи не зможуть повністю захистити громадян від шахрайства, якщо вони самі не будуть активними у захисті своїх прав та інтересів. У цьому контексті роль держави в подоланні цієї проблеми є надзвичайно важливою.

Отже, держава повинна реалізувати стратегію, спрямовану на вдосконалення та узгодження фінансових інтересів усіх учасників економічної діяльності. З цією метою доцільно розробити комплексний план боротьби з фінансовими шахрайствами, посилити ресурси та кадрове забезпечення для протидії цій проблемі, а також перенаправити державну фінансову політику не лише на компенсацію збитків громадянам і державі, а й на створення умов для попередження виникнення шахрайських схем у майбутньому.

Запобігання фінансовим шахрайствам потребує всебічного підходу, який включає технологічні, освітні та законодавчі заходи. Нижче наведено основні стратегії, які можуть сприяти зменшенню ризиків фінансового шахрайства:

- освіта та підвищення обізнаності. Необхідно впроваджувати програми фінансової грамотності для громадян і підприємців, а також організовувати інформаційні кампанії, спрямовані на ознайомлення з поширеними шахрайськими схемами та способами захисту від них;

- кібербезпека. Важливо використовувати сучасне антивірусне програмне забезпечення, регулярно оновлювати його, створювати складні паролі, застосовувати двофакторну аутентифікацію та бути обережними під час передачі особистої інформації в мережі;

- удосконалення фінансових сервісів. Варто вибирати лише перевірені фінансові платформи й банки, а також застосовувати системи моніторингу, здатні оперативно виявляти підозрілі або незвичайні фінансові операції;

- співпраця між фінансовими установами та правоохоронними органами. Необхідно забезпечити ефективний обмін інформацією про злочинну діяльність, а також створити умови для взаємодії між компаніями та секторами для передачі досвіду і впровадження найкращих практик;

- захист прав клієнтів. Важливо розробити механізми, які дозволяють клієнтам отримувати компенсацію у випадках шахрайства, а також забезпечити якісну підтримку для оперативного вирішення проблем, пов'язаних із підозрілими фінансовими операціями;

- удосконалення законодавчої бази. Варто запроваджувати і модернізувати правові акти, які спрямовані на запобігання фінансовим злочинам та покарання за них, а також розглянути використання технологій на основі блокчейну для підвищення безпеки фінансових операцій [27].

Ці стратегії взаємодіють між собою, формуючи цілісну систему заходів, спрямованих на запобігання фінансовим шахрайствам. Це сприяє підвищенню рівня безпеки та довіри у фінансовому середовищі. Однак найбільш дієвий

захист від шахрайства – це власна фінансова грамотність. Кожен має відповідати за збереження своїх коштів і конфіденційність персональних даних [37].

Для підвищення обізнаності громадян щодо боротьби з кібершахрайством Національний банк України спільно з платформою «Опентабот» започаткував масштабний освітній проєкт. Він є частиною інформаційної кампанії, мета якої – протидіяти платіжному шахрайству. У межах ініціативи також проводиться опитування користувачів, щоб визначити, як часто вони стикаються з кібершахрайством в умовах воєнного стану.

Згідно зі Стратегією розвитку фінансового сектору України, планується реалізація інформаційно-освітніх заходів, орієнтованих на різні цільові групи. Зокрема, буде створено єдину комунікаційну платформу, яка надаватиме важливу інформацію про фінансові послуги та правила їх використання. Також заплановано впровадження спеціалізованих програм для підвищення обізнаності громадян щодо користування фінансовими продуктами. Передбачається, що Міністерство цифрової трансформації розробить освітню ініціативу, спрямовану на підвищення цифрової грамотності у фінансовій сфері. Крім того, планується створення компетентнісних рамок фінансової грамотності, які охоплюватимуть різні вікові категорії – від дітей та молоді до дорослого населення [31].

У процесі створення механізму протидії криміналізації економіки важливо визначити ключових учасників, окреслити основи цього механізму, його складові, а також обрати відповідні підходи й методи для боротьби з криміналізацією. Основними елементами структури механізму протидії фінансовому шахрайству:

- нормативно-правова діяльність - створення законодавчої та нормативної бази для регулювання економічних процесів;

- правозастосовна та правоохоронна діяльність - реалізація та виконання законів, а також забезпечення дотримання правового порядку через правоохоронні органи;

- системний складник - підтримка стабільності та гармонії в елементах господарського механізму, зокрема в разі необхідності реформування системи управління макроекономікою та держуправлінням, якщо існують деструктивні елементи в її трансформації;

- організаційно-управлінський складник - включення організаційно-економічних заходів для ефективного управління та впливу на економічні процеси [28].

Інституціональні основи цього механізму складаються з:

- системи правових інститутів - формування норм права, законодавчої бази для регулювання економічної діяльності, а також системи органів, що здійснюють реалізацію норм і охорону правового порядку;

- системи економічних відносин - розвиток та регулювання економічних взаємодій між учасниками ринку;

- економічних інститутів управління макроекономікою - створення інститутів, що забезпечують ефективне управління на макрорівні економіки [26].

Важливим елементом механізму протидії фінансовому шахрайству є визначення основних етапів його формування. До таких етапів можна віднести кілька ключових кроків:

- аналіз та дослідження проблеми;
- розробка науково обґрунтованих і методологічних засад політики боротьби з шахрайством у бізнес-середовищі та економічному управлінні національною економікою;

- створення концепції механізму протидії шахрайським явищам у бізнесі та економічному управлінні;

- формулювання концептуальних підходів до інституційних та функціональних основ цього механізму;

- підготовка і реалізація програми або політики, спрямованої на боротьбу з шахрайством у бізнес-секторі та економічному управлінні.

- виконання зовнішніх програм, які забезпечують створення нової моделі національної економічної системи, нових підходів до макроекономічного управління та економічної поведінки, що дозволяють сформувати інституційні та інші умови для мінімізації кримінальних явищ, зокрема економічного шахрайства [28].

В Україні не існує єдиного нормативного регулювання фінансового шахрайства, що призводить до наявності численних суперечностей між різними положеннями окремих нормативних актів. Це створює умови для маніпулювання нормами законодавства і сприяє розвитку шахрайства.

На відміну від цього, у міжнародній практиці використовується цілий набір інструментів для управління ризиками, пов'язаними з фінансовим шахрайством. Зокрема, застосовуються такі інструменти:

- комплаєнс – набір внутрішніх політик, норм і положень, яких зобов'язані дотримуватися всі співробітники компанії. В розвинених західних країнах система комплаєнс контролюється на рівні держави, і її порушення часто веде до адміністративного чи кримінального покарання. В Україні ж компанії здебільшого орієнтуються тільки на свої внутрішні правила;

- аудит фінансової звітності – процедура, що дозволяє перевірити прозорість та достовірність фінансових операцій, відображених у бухгалтерії, порівнюючи їх з первинними документами. В багатьох компаніях використовуються програми, такі як 1С чи SAP. Головною метою аудиту є підвищення довіри до фінансової звітності компанії;

- система оповіщення про порушення – це механізм зворотного зв'язку, що дозволяє виявляти шахрайство завдяки повідомленням від працівників підприємства. Така система є важливим інструментом для реалізації політики нульової толерантності до будь-якого виду шахрайства в компанії;

- внутрішні інструменти – компанії використовують зовнішнього фінансового контролера, який підпорядковується безпосередньо акціонерам

чи власникам. Цей контролер є незалежним і незаангажованим, що робить його більш ефективним у порівнянні з корпоративною безпекою або внутрішнім аудитом [25].

Однак світова практика свідчить, що найбільш ефективні методи боротьби з економічною злочинністю, якщо їх застосовувати комплексно та регулярно.

Низький рівень ризику і високий потенціал прибутку від економічних злочинів роблять їх надзвичайно привабливими для організованих злочинних угруповань. Можливість виявлення шахрайства і притягнення злочинців до відповідальності залишається низькою через складність проведення розслідувань. Це особливо стосується випадків шахрайства, яке можна виявити лише через міжнародне співробітництво або ж у сфері інтернет-злочинів, де потрібно визначити юрисдикцію.

Щодо зменшення причин фінансового шахрайства, слід зазначити, що в цьому процесі необхідно:

- підвищувати рівень фінансової грамотності населення;
 - вдосконалювати регуляторні механізми;
 - впроваджувати технологічні інновації, серед яких вагоме місце на сьогодні займає штучний інтелект, що відіграє важливу роль у забезпеченні кіберзахисту, ставши новим інструментом у протистоянні цифровим загрозам;
 - здійснювати спільну боротьбу фінансових установ проти шахрайства.
- Для досягнення результату необхідно впроваджувати не лише індивідуальні рішення, а й створювати централізовану систему, яка б координувала зусилля та забезпечувала обмін інформацією між різними установами. Це дозволить ефективніше використовувати можливості ШІ та швидше реагувати на нові виклики [44];
- налагоджувати злагоджену взаємодію всіх структур, включаючи карний розшук, слідчі органи, кіберполіцію та підрозділи, що займаються кримінальним аналізом;

- сприяти розширенню взаємодії з банківськими організаціями, постачальниками послуг, Держспецзв'язком та Державною кримінально-виконавчою службою;
- удосконалювати механізм фіксації шахрайства та впровадження сучасних засобів протидії шахрайству;
- покращувати фінансову мотивацію працівників і забезпечувати відповідний рівень їх винагороди. Проте, при аналізі причин шахрайства не слід надмірно акцентувати на фінансових аспектах, оскільки важливу роль також відіграють моральні фактори, такі як страх перед покаранням або почуття сорому за нечесну поведінку;
- формувати вкрай негативне ставлення до неетичної професійної поведінки серед недобросовісних працівників, які можуть стати потенційними мотиваторами для шахрайства;
- усувати непрозорі схеми обліку та звітності, а також потенційні фінансові маніпуляції всередині компанії;
- застосовувати деперсоналізовані моделі кіберзахисту, що працюють на основі аналізу великих масивів даних. Ці моделі будуть здатні виявляти загрози, враховуючи унікальність кожної установи.

Захист від фінансового шахрайства - це не лише питання технологій, а й необхідність у тісній співпраці, централізованому підході та постійному вдосконаленні. Протидія економічній злочинності стає особливо важливою в умовах кризових періодів та воєнного часу. Постійні виклики глобального економічного середовища створюють нові можливості для шахрайських схем. На жаль, потрібно багато часу, щоб пристосуватися до змін, тоді як шахраї швидше знаходять способи використати ці зміни для власної вигоди. З огляду на те, що середній фінансовий збиток від шахрайських дій зростає в усьому світі, здатність ефективно на них реагувати набуває критичного значення. Використання відповідних технологій та впровадження конкретних заходів можуть допомогти усунути прогалини в системі боротьби з фінансовим шахрайством.

Висновки до 3 розділу

Аналіз міжнародного досвіду боротьби з фінансовим шахрайством є надзвичайно важливим у контексті сучасного розвитку української економіки, оскільки шахрайські схеми набувають нових, більш складних форм, що збільшують рівень корисливості та соціальної небезпеки, а також спричиняють зростання міжнародних злочинів. Варто зазначити, що проблема фінансових шахрайств не обмежується лише Україною. У ряді країн застосування шахрайських методів призвело до серйозних макроекономічних і соціально-політичних наслідків.

Досвід інших країн свідчить про те, що кожна цивілізована держава в умовах глобалізації намагається захистити свою фінансову систему від злочинних вторгнень. Для цього ефективними є заходи економічного, правового, морального та психологічного характеру, які мають важливе значення як у профілактиці, так і в компенсації наслідків. Це захист фінансового сектора, який не тільки оберігає інтереси фінансових установ і їхніх клієнтів, але й підтримує стабільність економіки країни загалом.

Основна увага у боротьбі з фінансовим шахрайством повинна бути зосереджена на його попередженні, тобто на усуненні умов, що створюють можливості для шахрайства. Це набагато ефективніше, ніж реагування на злочини та усунення їх наслідків. Врахування цього принципу є важливим при формуванні державної політики щодо зниження рівня фінансових шахрайств. Така політика повинна бути обґрунтована на наукових дослідженнях і практичному досвіді, мати комплексний підхід, що передбачає взаємодію фінансових установ і правоохоронних органів, а також активну участь громадянського суспільства. Крім того, ця політика має бути не лише реакцією на шахрайські дії, а й спрямованою на створення надійної профілактичної системи, що виключає можливість вчинення фінансових шахрайств.

ВИСНОВКИ

Кваліфікаційна робота присвячена аналізу проблеми фінансового шахрайства та розробці заходів його попередження. На основі проведеного дослідження сформульовано такі висновки:

Процеси глобалізації охопили всі аспекти економічної діяльності суспільства, включно з фінансовою сферою, що сприяє зростанню масштабів фінансового шахрайства та різноманітності його форм і схем. У результаті дослідження сутності цього явища було запропоновано його визначення: фінансове шахрайство – це негативний соціально-економічний феномен, розвиток якого зумовлений низкою економічних факторів. Ці фактори штовхають людей на пошук швидких і легких шляхів отримання доходів. Основними причинами поширення фінансового шахрайства є низький рівень фінансової грамотності населення, недостатнє розуміння наявних ризиків і загроз, жадоба до швидкого збагачення, підвищена мотивація до порушення закону та недостатній рівень суспільного осуду таких дій.

Процес виявлення та мінімізації ризиків фінансового шахрайства може здійснюватися через різноманітні методи, які враховують специфіку як зовнішнього, так і внутрішнього середовища. Ризик фінансового шахрайства визначається як імовірність його виникнення та наслідки, які можуть негативно вплинути на фінансову стійкість фізичних осіб, організацій або держави. Важливим етапом управління цими ризиками є їх ідентифікація, що передбачає аналіз основних типів ризиків, властивих діяльності певного суб'єкта, які здатні вплинути на його фінансовий стан або стратегічні цілі. Цей процес включає оцінку ризиків у контексті їх взаємозв'язку з іншими факторами чи джерелами, які можуть як підсилювати, так і знижувати імовірність їх реалізації.

Останнім часом спостерігається стрімке зростання рівня фінансового шахрайства, яке щороку набуває нових форм і масштабів. Це явище має складну економічну природу, яка спонукає людей до пошуку можливостей для

швидкого збагачення. Водночас недоліки чинного законодавства України створюють передумови для шахраїв розробляти нові способи обману, припускаючи, що покарання вдасться уникнути. У зв'язку з цим ключовим завданням є вдосконалення механізмів державного регулювання у сфері боротьби з фінансовим шахрайством.

Сьогодні фінансове шахрайство набуло значного поширення та продовжує активно розвиватися. Шахраї використовують широкий спектр методів обману, починаючи від простих схем і закінчуючи складними маніпуляціями. Найбільш популярними способами є встановлення спеціальних пристроїв на банкомати для незаконного зняття готівки, SMS-шахрайство, телефонні обмани, фішинг, шахрайські дії з криптовалютами, маніпуляції під час фінансових операцій, а також кібератаки із використанням вірусів і програм-вимагачів.

У 2023 році середній розмір однієї шахрайської операції склав 3065 гривень, що на 865 гривень більше, ніж у 2022 році. Порівняно з 2019 роком, коли цей показник становив 2100 гривень, спостерігається збільшення на 965 гривень. У 2023 році кількість шахрайських транзакцій із використанням платіжних карток зросла на 25%, досягнувши 272 тисяч випадків. Інтернет став основним середовищем для шахрайства, на яке припадало 83% усіх зафіксованих інцидентів, що трохи менше, ніж у 2022 році. У той же час частка злочинів, пов'язаних із фізичними пристроями, такими як банкомати та POS-термінали, збільшилася до 17%. В умовах повномасштабної війни в Україні кількість шахрайських злочинів різко зросла. У 2023 році за статтею 190 Кримінального кодексу України («Шахрайство») було відкрито 82 609 кримінальних проваджень, що стало рекордним показником за останні роки. Порівняно з 2022 роком кількість таких проваджень зросла у 2,6 раза.

Досвід зарубіжних країн у протидії фінансовому шахрайству є цінним джерелом для України, оскільки він надає ефективні механізми, превентивні заходи та методи боротьби з цим явищем. Хоча Україна поки що не належить до економічно розвинених країн, вона активно працює над вдосконаленням

своїї економічної системи, прагнучи стати конкурентоспроможною на міжнародній арені. На сьогоднішній день форми фінансового шахрайства стали більш складними та різноманітними, а кількість злочинів, пов'язаних із незаконними операціями, значно зросла. Особливо турбує зростання кількості злочинів, що мають міжнародний характер, адже шахрайські схеми часто організовуються групами, до складу яких входять громадяни різних держав.

Сучасна політична й соціально-економічна нестабільність в Україні створює сприятливе середовище для розповсюдження шахрайських дій. Попри значний негативний вплив на економіку та суспільство, проблема фінансового шахрайства залишається недостатньо вивченою, що частково обумовлено відсутністю чітко сформульованих законодавчих норм, спрямованих на боротьбу з цим явищем. Варто зазначити, що навіть прийняття нових законів або проведення економічних реформ не гарантує повного захисту населення від шахрайських дій, якщо самі громадяни не будуть брати активну участь у захисті своїх прав і фінансових інтересів. У зв'язку з цим ключова роль у вирішенні цієї проблеми покладається на державу. Державна політика повинна бути спрямована на впровадження стратегії, яка сприятиме гармонізації фінансових інтересів усіх учасників економічних процесів. Для цього необхідно розробити комплексний підхід до боротьби з фінансовим шахрайством, посилити ресурсну базу та кадрове забезпечення органів, що займаються протидією шахрайству. Водночас слід переорієнтувати державну фінансову політику не лише на відшкодування збитків, але й на створення умов для запобігання виникненню шахрайських схем у майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абрамєйцева Є.А. Види фінансового шахрайства. *Фінансове право*. 2020. № 3. С. 45–52.
2. Безділь Н.Б., Данилюк М.М., Дмитришин М.В. Ідентифікація та мінімізація ризиків фінансового шахрайства під час прийняття управлінських рішень. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/4289/4214>.
3. Всесвітнє дослідження економічних злочинів та шахрайства 2020: результати опитування українських організацій. URL: <https://www.pwc.com/ua/uk/survey/2020/gecs-ua-2020-ukr.pdf>
4. Все про шахрайські схеми в бізнесі та шахраїв! Частина 1. URL: <https://cutt.ly/CNzNS8A>
5. Державна аудиторська служба України. URL: https://uk.wikipedia.org/wiki/%D0%94%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%BD%D0%B0_%D0%B0%D1%83%D0%B4%D0%B8%D1%82%D0%BE%D1%80%D1%81%D1%8C%D0%BA%D0%B0_%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D0%B0_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8.
6. Дмитришин М. В., Панчак Н. В. Удосконалення політики управління кредитним портфелем ПАТ КБ ПриватБанк на основі SWOT-аналізу кредитного портфелю комерційного банку. *Економічний вісник університету*, 2016. № 28 (1). С. 165–171.
7. Дмитришин М. В., Данилишин М.М. Формування системи ефективного управління фінансовими ресурсами підприємства. *Актуальні проблеми розвитку економіки регіону*. 2015. № 11 (2). С. 131–138.
8. Запобігання корупції у приватному секторі: монографія / [В. С. Батиргарєєва, Б. М. Головкін, О. В. Новіков та ін.]; за заг. ред. Б. М. Головкіна. Харків: Право, 2020. 286 с.

9. Економічні злочини у період кризи Всесвітній огляд динаміки економічної злочинності. PricewaterhouseCoopers. URL: <https://cutt.ly/XNLE0F1>
10. Кізима Т., Хамига Ю. Фінансове шахрайство: Теоретична концептуалізація та економічне підґрунтя. URL: <http://sf.wunu.edu.ua/index.php/sf/article/view/1230>.
11. Коновалова І. О. Досвід запобігання шахрайству в сфері електронної торгівлі в США. *Науковий вісник Ужгородського Національного Університету*, 2021. С. 220–224.
12. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>
13. Кравченко О. В. Психологічні особливості шахрайства : автореф. дис. ... канд. психол. наук : спец. 19.00.06 / Нац. ун-т внутр. справ. Харків, 2005. 21 с.
14. Майже утричі скоротилася кількість нових справ за шахрайство від початку року. URL: <https://opendatabot.ua/analytics/fraud-2024-8>.
15. Мельник О. Г. Міжнародний досвід запобігання та протидії корупції як вектор формування національної антикорупційної політики в Україні. *Юридичний науковий електронний журнал*. 2021. № 2. С. 32–35.
16. Мудряк Т. О. Особливості розслідування шахрайства з фінансовими ресурсами. *Міжнародний юридичний вісник : зб. наук. праць Нац. ун-ту державної податкової служби України*. 2014. Вип. 1. С. 128–133.
17. Надавачі платіжних послуг мають застосовувати посилену автентифікацію користувачів. URL: <https://bank.gov.ua/ua/news/all/z-metoyu-znijennya-rizikiv-shahraystva-nadavachi-platijnih-poslug-zastosuvatimut-posilenu-avtentifikatsiyu-16500>.
18. Найімовірніші шахрайства, яких слід остерігатися у 2024 році. URL: <https://www.scamadviser.com/uk/articles/nayimovirnishi-shakhraystva-iakykh-slid-osterihatysia-u-2024-rotsi>.

19. Національна стратегія розвитку фінансової грамотності до 2030 року. URL: <https://bank.gov.ua/ua/news/all/zatverdjeno-natsionalnu-strategiyu-rozvitku-finansovoyi-gramotnosti-do-2030-roku>.
20. Нежива М.О., Мисюк В.О. Протидія шахрайству в умовах війни. *Бізнес Інформ*. 2023. № 1. С. 160–166.
21. Операція «Еврика»: правоохоронці заарештували членів мафіозного синдикату «Ндрангета». URL: <https://www.rfi.fr/uk/міжнародні-новини/20230503-операція-еврика-правоохоронці-заарештували-членів-мафіозного-синдикату-ндрангета>.
22. Офіційний сайт НБУ. URL: <https://bank.gov.ua/>.
23. Офіційний сайт Державної податкової служби. URL: <https://tax.gov.ua/>.
24. Офіційний сайт Міністерства фінансів України. URL: <https://mof.gov.ua/uk/>.
25. Офіційний сайт Міністерства економіки України. URL: <http://www.me.gov.ua>.
26. Підприємницьке право України : підручник / ра заг. ред. доц. Р.Б. Шипки. Харків : Еспада, 2000. 480 с.
27. Рєзнік О.М., Болгов Г.О. Фінансове шахрайство: сутність та заходи протидії. URL: http://essuir.sumdu.edu.ua:8080/bitstream-download/123456789/94144/1/Reznik_Financial_fraud.pdf
28. Руснак Л.Р. Концептуальні засади розроблення цільової програми протидії фінансовому шахрайству. URL: https://economyandsociety.in.ua/journals/10_ukr/21.pdf.
29. Сахневич С. Ключові фактори виникнення фінансових маніпуляцій, пірамід та масових спекуляцій. URL : <http://innovations.com.ua/ua/articles/14390/temp>
30. Словник української мови: в 11 т. / АН УРСР, Інститут мовознавства; за ред. І. К. Білодіда. К.: Наукова думка, 1970–1980. Т. 11. С. 423.

31. Стратегія розвитку фінансового сектору України. URL: https://bank.gov.ua/admin_uploads/article/Strategy_finsector_NBU.pdf?v=11.
32. Сухонос В. В. Шахрайство з фінансовими ресурсами у банківській сфері України та його кримінологічна характеристика. *Вісник прокуратури*. 2012. № 1. С. 92-96.
33. Товкун Л.В. Правове регулювання фінансових технологій: аналіз національного та світового досвіду. URL: http://www.lsej.org.ua/6_2024/66.pdf.
34. Угода про асоціацію України з Європейським Союзом від 27.06.2014 р. URL: http://eeas.europa.eu/delegations/ukraine/eu_ukraine/association_agreement/index_uk.htm.
35. Феномен фінансових пірамід. Експерти радять захищатися від подібних шахрайських схем самостійно. URL : <http://www.kreschatic.kiev.ua/print/art/1346179696.html>
36. Фінансове шахрайство та його особливості у роздрібному і корпоративному сегментах. URL: <https://finclub.net/priama-mova/finansove-shakhraistvo-ta-ioho-osoblyvosti-u-rozdribnomu-i-korporatyvnomu-sehmentakh.html>
37. Фінансове шахрайство та особиста фінансова безпека. Офіційний вебсайт. URL: https://elib.lntu.edu.ua/sites/default/files/elib_upload/%D0%A4%D0%86%D0%BD%D0%B0%D0%BD%D1%81%D0%BE%D0%B2%D0%B0%20%D0%B3%D1%80%D0%B0%D0%BC%D0%BE%D1%82%D0%BD%D1%96%D1%81%D1%82%D1%8C%20%D0%95%D0%9D%D0%9F/page15.html.
38. Франк С., Пол В. Розуміння жертв шахраїв: сім принципів безпеки систем. *Комунікації АСМ*. 2017. № 54(3). С. 70–75.
39. Хамига Ю. Я. Фінансове шахрайство: критерії ідентифікації та напрями мінімізації : дис. ... д-ра філос. : 072 Фінанси, банківська справа та страхування. Тернопіль : ЗУНУ, 2020. 284 с.
40. Чернишов Г. М. Фінансове шахрайство як злочинна діяльність: методологічні проблеми дослідження. *Актуальні проблеми держави і права*. 2013. Вип. 70. С. 369-376. URL: http://nbuv.gov.ua/UJRN/apdp_2013_70_58.

41. Чернявський С. С. Наукові основи розробки криміналістичної методики розслідування фінансового шахрайства. *Науковий вісник Київського національного університету внутрішніх справ*. 2008. № 6. С. 89–100.
42. Чорнуцький С. П. Суть і методика виявлення фактів фінансового шахрайства. *Економіка та держава*. 2011. № 7. С. 127–131.
43. Шахрайство з криптовалютою: схеми, захист, запобіжні заходи. URL:<https://minfin.com.ua/ua/crypto/articles/shahraystvo-z-kriptomalyutoyu-shemi-zahist-zapobizhni-zahodi/>
44. Шахрайство на фінансовому ринку: теперішні і майбутні виклики. URL:<https://epravda.com.ua/columns/2024/07/3/716052/>.
45. Шахраї не сплять: у 2023 році з карток українців викрадено понад 800 млн. гривень. URL:<https://mind.ua/publications/20271695-shahrayi-ne-splyat-u-2023-roci-z-kartok-ukrayinciv-vikradeno-ponad-800-mln-griven>.
46. 2022 Annual Fraud Report. URL:
https://www.ukfinance.org.uk/system/files/2023-05/Annual%20Fraud%20Report%202023_0.pdf.
47. Brian O'Connell. 9 of the Biggest Financial Fraud Cases in History. 2023. URL: <https://money.usnews.com/investing/stock-market-news/slideshows/biggestcorporate-frauds-in-history>.
48. 10 Common Types of Financial Fraud & Schemes URL:
<https://www.aura.com/learn/types-offinancial-frauds>.
49. Danyliuk M., Dmytryshyn M., Goran T. Informatization in Ukraine: Realities, problems, prospects. *European Journal of Sustainable Development*, 2021. № 10(4). P. 190–202.
50. 2021 Identity fraud report shifting angles identity fraud. URL:
<https://javelinstrategy.com/content/2021-identity-fraud-report-shifting-angles-identity-fraud>.
51. International Standard on Auditing 240: The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements. URL:

<http://www.ifac.org/sites/default/files/downloads/a012-2010-iaasb-handbook-isa-240.pdf>

52. Opération Eurêka: 25 perquisitions et 13 personnes arrêtées en Belgique au cours d'une des plus grosses opérations antimafia jamais menées en Europe. URL: <https://www.rtb.be/article/operation-eureka25-perquisitions-et-6-personnes-arretees-en-belgique-au-cours-dune-des-plus-grosses-operations-antimafiajamais-menees-en-europe-11192185>.

53. Over £1.2 billion stolen through fraud in 2022, with nearly 80 per cent of APP fraud cases starting online. URL: <https://www.ukfinance.org.uk/news-andinsight/press-release/over-ps12-billion-stolen-throughfraud-in-2022-nearly-80-cent-app>.

54. Top Trends to watch out for in 2023 regarding fraud and financial crime. URL: <https://quadrant-solutions.com/blogs/top-trends-to-watch-out-for-in-2023-> regarding-fraud-and-financial-crime.