

УДК 343.72:004(477)

DOI: <https://doi.org/10.33098/3083-726X.2025.1.32.183-189>

ПРОБЛЕМИ ОБЛІКУ ТА ПРОТИДІЇ ШАХРАЙСТВУ В КОНТЕКСТІ СУЧАСНИХ ВИКЛИКІВ

Микитюк Вікторія*, Пташник Олександра**,

*студентка IV курсу спеціальності «Право», ЗВО «Університет Короля Данила» (м. Івано-Франківськ, Україна)

**в.о.завідувача кафедри права ім. акад. УАН о.І.М.Луцького, кандидат соціологічних наук, доцент, ЗВО «Університет Короля Данила» (м. Івано-Франківськ, Україна) ORCID: <https://orcid.org/0000-0002-1529-2443>

Метою дослідження є аналіз тенденцій обліку кримінальних правопорушень за ознаками шахрайства в Україні у контексті сучасних викликів, зокрема воєнного стану та стрімкої цифровізації суспільства. У статті досліджено динаміку шахрайств за останні роки, виявлено основні проблеми, що впливають на достовірність статистичних даних та ефективність розслідування. Зокрема, розглянуто різноманітні види інтернет-шахрайства, такі як фішингові повідомлення, фейкові благодійні збори та махінації з міжнародною допомогою. Автор звертає увагу на практичні аспекти розмежування складів злочинів при використанні комп'ютерних технологій, що вказує на потребу в удосконаленні правозастосовних підходів. Наукова новизна полягає в актуалізації проблеми латентності шахрайства в умовах посилення його цифрових форм та воєнного стану, а також в обґрунтуванні необхідності системного підходу до протидії цьому явищу. Запропоновано комплекс заходів, що включає розвиток превентивного моніторингу з використанням штучного інтелекту, створення єдиного реєстру кіберзлочинів та впровадження етичного хакінгу для виявлення та усунення вразливостей у системах безпеки. Результати дослідження можуть бути використані для вдосконалення чинного законодавства, розробки ефективних стратегій боротьби з кіберзлочинністю та підвищення обізнаності громадян щодо сучасних шахрайських схем.

Ключові слова: шахрайство, кіберзлочинність, статистика злочинності, протидія злочинності, фішинг, етичний хакінг, превентивний моніторинг, латентна злочинність, банківське шахрайство.

© Микитюк В., Пташник О., 2025

Стаття поширюється на умовах ліцензії CC BY 4.0

Микитюк В., Пташник О. Проблеми обліку та протидії шахрайству в контексті сучасних викликів. *Art of Justice*. Редакційно-видавничий відділ Університету Короля Данила, 2025. Вип. 1 (32). С. 183-189. DOI: <https://doi.org/10.33098/3083-726X.2025.1.32.183-189>

Постановка проблеми

У сучасних умовах проблема шахрайства набуває особливої гостроти, зважаючи на трансформаційні процеси в соціально-економічній, політичній та цифровій сферах. В умовах воєнного стану, нестабільної економіки, стрімкого розвитку цифрових технологій та зростання онлайн-середовища, способи вчинення шахрайства суттєво ускладнюються та набувають нових форм. Зокрема, спостерігається зростання кіберзлочинності, фінансових махінацій, шахрайських схем у сфері благодійної допомоги, електронної комерції, банківських операцій та соціальних виплат.

Разом з тим, згідно з даними офіційної статистики за 2024 рік, спостерігається зменшення кількості облікованих проваджень за ознаками шахрайства. Однак, хоча кількість облікованих випадків шахрайства знижується, та реальний рівень безпеки громадян не демонструє покращення. Це свідчить про можливі проблеми у веденні обліку злочинів та їхньої реєстрації, що може сприяти безкарності злочинців та формуванню умов для зростання тіньової злочинності. А це, у свою чергу, ускладнює боротьбу з

правопорушеннями. Крім того, штучне зменшення статистичних показників може бути використане як інструмент впливу на суспільну думку.

Таким чином, недостатня ефективність механізмів попередження, виявлення та притягнення винних до відповідальності свідчить про наявність істотних прогалин як у чинному законодавстві, так і в практиці його застосування. Особливої уваги потребує питання вдосконалення правових норм, що регламентують кваліфікацію шахрайства в умовах цифровізації, а також узгодження кримінального законодавства з новітніми викликами.

Аналіз останніх досліджень та публікацій

Аналізом окремих питань протидії шахрайства займаються О. М. Брисковська, М. О. Гелемей (Брисковська, Гелемей, 2023), М. В. Карчевський (Карчевський), Т. В. Коршикова, Я. В. Левківська, Д. О. Ричка, С. В. Самойлов, Р. А. Усманов (Усманов), І. М. Чекмарьова (Чекмарьова), М. Г. Фортунатова (Фортунова, Мусієнко) та інші.

Постановка завдання

Визначити тенденції обліку кримінальних правопорушень за ознаками шахрайства в Україні у 2024 році, дослідити та знайти важелі врегулювання покарань за вчинені злочини, а також розробити рекомендації щодо вдосконалення системи реєстрації правопорушень.

Виклад основного матеріалу дослідження

Аналіз статистичних показників останніх років свідчить про безпрецедентне зростання кількості шахрайських дій в Україні, що прямо корелює з повномасштабним вторгненням та міграцією злочинності в кіберпростір. Згідно з даними Офісу Генерального прокурора та аналітикою сервісу «Опендатабот», 2023 рік став піковим за кількістю відкритих кримінальних проваджень за ст. 190 КК України («Шахрайство») — було зареєстровано понад 82,6 тисяч справ. Цей показник став найвищим за останні 11 років, перевищивши дані 2021 року у 2,6 рази¹.

У 2024 році спостерігається певна тенденція до зниження абсолютної кількості зареєстрованих проваджень — близько 64 978 справ, що на 21% менше порівняно з рекордним 2023 роком. Проте, навіть цей «знижений» показник залишається у 2,7 рази вищим, ніж у довоєнний період. Варто зазначити, що попри величезний масив відкритих проваджень, показник справ, що доходять до суду, залишається критично низьким: у 2023 році він становив лише 18%, а у 2024 році зріс до 24%².

Особливу занепокоєність викликає структура цих злочинів. За даними Національного банку України, переважна більшість випадків платіжного шахрайства (83%) відбувається саме в мережі Інтернет. У 2023 році сума збитків від незаконних дій з платіжними картками зросла на 73% і сягнула 833 мільйонів гривень. Середня сума однієї незаконної операції зросла до 3065 грн³. Це підтверджує тезу про те, що сучасне шахрайство трансформувалося з вулично-побутового злочину у високотехнологічну індустрію, де використовуються методи соціальної інженерії та фішингу.

¹ В Україні рекордно зросла кількість справ про шахрайство // Опендатабот. 2024. URL: <https://opendatabot.ua/analytics/fraud-2023>.

² Шахрайства в Україні: підсумки 2024 року // Опендатабот. 2025. URL: <https://www.google.com/search?q=https://opendatabot.ua/analytics/fraud-2024>.

³ Сума збитків від шахрайства у 2023 році зросла на 73% — НБУ // Офіційне інтернет-представництво Національного банку України. URL: <https://bank.gov.ua/ua/news/all/prichinoyu-bilshosti-shahrayskih-vipadkiv-z-platijnimi-kartkami-stalo-rozgoleshennya-danih-yihnimi-koristuvachami>.

Такі статистичні дані вказують на дві ключові проблеми обліку та протидії: по-перше, високий рівень латентності (значна частина потерпілих не звертається до поліції через невеликі суми збитків або зневіру), а по-друге, складність розслідування кіберзлочинів, що призводить до низького відсотка передачі справ до суду.

Зафіксоване у 2024 році значне зниження кількості облікованих шахрайських правопорушень, може бути наслідком як реального покращення криміногенної ситуації, так і змінами у методології реєстрації злочинів. Особливу увагу привертає можливе виключення значної частини шахрайських випадків із офіційної статистики, що може свідчити про недостатню ефективність правозастосовної практики та наявність проблем у зборі доказів, особливо у сфері кіберзлочинності. Крім того, дослідження показують, що традиційні форми шахрайства поступово замінюються цифровими схемами, що ускладнює їхнє виявлення та притягнення винних до відповідальності (Карчевський).

Це небезпечно тим, що викривлена статистична картина може сприяти ілюзії зниження злочинності та, відповідно, зменшенню уваги державних органів до проблеми шахрайства. Недостатній облік таких злочинів може створювати умови для безкарності зловмисників, що лише стимулюватиме їхню подальшу злочинну діяльність. Крім того, громадяни можуть недооцінювати реальні ризики шахрайства, що призведе до збільшення кількості жертв. Особливу загрозу становить кіберзлочинність, яка дедалі більше ускладнюється використанням анонімних цифрових технологій та відсутністю єдиної стратегії боротьби з нею.

Для сучасного суспільства характерним є стрімкий розвиток інформаційних технологій. І тому варто врахувати факт того, що з розвитком будь-якої ніші суспільства, можуть вчинятися кримінальні правопорушення. Це стосується і вчинення злочинів за допомогою комп'ютерних технологій. Відповідно, питання щодо проблеми судової практики є дуже поширеним, і подібні злочини в багатьох випадках мають різну кримінально-правову оцінку, тобто, деякі випадки кваліфікуються як крадіжка ст.185 ККУ¹, інші - шахрайство ст.190 ККУ², що вказує на необхідність уніфікації правозастосовних підходів. У таких видах шахрайства застосовуються різні види обману, наприклад опосередкований чи технічно опосередкований, які полягають у введенні в оману банківської чи платіжної системи без контакту з жертвою або ж використання технологій для маніпуляцій фінансовими операціями. Таким чином, ці злочини часто вважаються латентними, тим самим послаблюється дотримання принципу невідворотності покарання та значно знижується довіра до правоохоронних органів.

Якщо брати до уваги статистичні дані щодо облікованих випадків шахрайства у 2023 та 2024, то у порівнянні з 2023 роком, кількість таких посягань у 2024 зменшилась. Водночас, спостерігається збільшення шахрайства, як наслідок розширення сфери застосування інтернет та дистанційних систем банківського обслуговування. Зокрема поява нових схем, шахрайських кол-центрів, які видають себе за представників банків чи державних установ (Карчевський). Особливого поширення шахрайство в інтернеті набуло з введенням воєнного стану. Брисковська О. М. та Гелемей М. О., аналізуючи особливості вчинення шахрайства в мережі інтернет, акцентують на великій поширеності такого різновиду зазначеного злочину, як хибні інтернет повідомленнях. Вони виокремлюють такі їх різновиди, як: тиск терміновістю, коли шахраї навмисне використовують слова на

¹ Кримінальний кодекс України. Закон України від 01.02.2025 Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131 URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

² Кримінальний кодекс України. Закон України від 01.02.2025 Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131 URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

кшталт «негайно» чи «терміново», щоб викликати емоційну реакцію та змусити людину клікнути на підозріле посилання або відповісти на лист. Часто такі повідомлення імітують стиль банків, компаній чи знайомих, імітуючи проблеми з рахунком або обіцяючи бонуси; залякування зламом - повідомленням про небезпеку щодо безпеки акаунтів чи паролів; фальшиві «приємні новини» - позитивно оформлені листи, які обіцяють вигідні пропозиції або виграші; прохання змінити пароль; фіктивні збори на армію - виманювання коштів нібито на ЗСУ, зокрема через звернення, які виглядають як запити від керівництва військових адміністрацій; організовані схеми вимагання під виглядом благодійності; шахрайські збори через соцмережі; псевдоблагодійні організації; обман із міжнародною допомогою - через підроблений чат-бот зловмисники запрошували громадян отримати грошову підтримку, перенаправляючи їх на фішингові сайти для збору банківських даних; оголошення про продаж транспорту; зловживання довірою до банків - під виглядом банківських працівників злочинці випитують персональні коди клієнтів, отримуючи доступ до рахунків, з метою переведення коштів; фіктивна оренда житла; обмани з полоном - громадянам телефонували з фейковими історіями про родичів у полоні та вимагали викуп за "звільнення"; шахрайство на основі даних про зниклих - особи контактують з рідними зниклих, обіцяючи за винагороду повідомити їх місцеперебування; онлайн-обмани в інтернет-магазинах - отримання передплати без доставки, продаж неякісного або підмінного товару, невиконання зобов'язань з боку продавця (Брисковська, Гелемей, 2023).

Це також ускладнює збір доказів, особливо в кіберзлочинах, де злочинці можуть працювати з-за кордону та використовувати анонімні канали зв'язку. Відповідно, якщо раніше спостерігалось домінування звичайних майнових злочинів, то зараз на перший план виходять шахрайства з активним використанням цифрових технологій. Кількість засуджених за цією статтею значно менша, ніж загальна кількість облікованих злочинів, що вказує на труднощі зі збором доказів, недостатньою координацією між правоохоронними органами та невисокий рівень обізнаності потерпілих у фінансових і цифрових питаннях.

Дослідивши роботи М. Карчевського (Карчевський), зокрема CrimeDataLab – аналіз статистики протидії злочинності (Рисунок 1), прослідковується потреба щодо вдосконалення обліку шахрайства та підвищення ефективності боротьби з ними.

Необхідним, насамперед, є розвиток превентивного моніторингу, а саме:

- 1) використання штучного інтелекту, для виявлення підозрілих дій у кіберпросторі;
- 2) впровадження систем раннього попередження, які автоматично зможуть інформувати користувачів про можливу загрозу, що сприятиме зменшенню кількості успішних шахрайських схем.

Далі, не менш важливим кроком, є створення єдиного реєстру кіберзлочинів, який буде ефективним інструментом для швидкого реагування правоохоронними органами на випадки шахрайства, за рахунок прогнозування майбутніх і аналізу тенденцій минулих загроз. І також запровадити етичний хакінг, який полягатиме у виявленні вразливості у системах безпеки та сприятиме їх усуненню.

Таким чином ці три аспекти утворять певну систему, яка дозволить вдосконалити облік шахрайства та ефективно впливатиме на боротьбу з цим видом кримінальних правопорушень.



Рисунок 1. Графік зменшення кількості шахрайства

Отже, зменшення кількості облікованих кримінальних правопорушень, передбачених ст. 190 КК України, не є свідченням зниження поширеності шахрайства, а, найімовірніше, вказує на викривлення статистичної картини з формальних причин, через оновлення законодавства. Водночас, умови воєнного стану, стрімкий розвиток цифрових технологій та зростання онлайн-комунікацій стали каталізаторами появи нових, більш складних шахрайських схем, що активно використовуються зловмисниками у кіберпросторі.

Типовими ознаками сучасних фор шахрайства є технічно опосередкований обман та відсутність фізичного контакту з потерпілим. Це значно ускладнює кримінально-правову протидію таким посяганням.

Встановлено, що розмежування між нормами ст. 185 та 190 КК України у випадках вчинення шахрайства із застосуванням комп'ютерних технологій викликає складнощі у правозастосовній практиці, що вимагає законодавчого врегулювання. Виявлено потребу в оновленні підходів до протидії шахрайству шляхом запровадження єдиного реєстру кіберзлочинів, розвитку превентивного моніторингу, впровадження систем раннього попередження та використання технологій штучного інтелекту й етичного хакінгу.

Висновки

Результати дослідження підтверджують, що прогрес інформаційних технологій створює нові виклики у протидії злочинності, зокрема кіберзлочинам та шахрайським схемам із використанням цифрових технологій. Аналіз наукових праць та практики правозастосування вказує на потребу вдосконалення законодавства щодо регулювання кіберзлочинів, зокрема визначення меж між традиційним шахрайством і злочинами, що здійснюються за допомогою комп'ютерних технологій. Вирішення проблем правової класифікації шахрайських дій та їхньої латентності вимагає підвищення ефективності

правоохоронної діяльності шляхом створення централізованих реєстрів кіберзлочинів і покращення взаємодії між державними установами. Важливим також є запровадження превентивного моніторингу з використанням штучного інтелекту для ідентифікації підозрілих дій та впровадження систем раннього попередження про потенційні загрози.

Додатковий внесок у зміцнення кібербезпеки може забезпечити етичний хакінг, спрямований на виявлення та усунення вразливостей у цифрових системах, що зменшить ризики шахрайських дій. Комплексний підхід, який включає законодавчі зміни, використання технологічних рішень та підвищення цифрової грамотності населення, сприятиме ефективнішій боротьбі з кіберзлочинами, захисту прав громадян і забезпеченню порядку в цифровому суспільстві.

Список використаних джерел

1. Брисковська О.М., Гелемей М. О. Особливості вчинення шахрайства в мережі Інтернет в умовах воєнного стану. *Київський часопис права*. 2023. No 3. С.174-180.
2. Карчевський, М. Протидія злочинності в Україні: інфографіка (2023-2024): інтерактивний довідник. *CrimeDataLab*. URL: <https://crimedatalab.org/>
3. Усманов Р.А. Деякі питання об'єктивної сторони шахрайства, вчиненого шляхом незаконних операцій з використанням ЕОТ. *Правничий часопис Донецького національного університету імені Василя Стуса*. (Вер 2024), 223-229. DOI: <https://doi.org/10.31558/2786-5835.2024.1.22>.
4. Усманов Р. А. Кримінальна відповідальність за шахрайство, вчинене шляхом незаконних операцій із використанням комп'ютерної техніки: дисертація. URL: <https://dnuvs.ukr.education/wp-content/uploads/2025/02/dysertac>
5. Фортунова М. Г., Мусієнко А.В. Актуальні аспекти запобігання латентній злочинності. *Dictum Factum*. С.283-306 URL: <https://df.duit.in.ua/index.php/dictum/article/view/366>
6. Чекмарьова І.М. Шахрайство в інтернеті як один із видів шахрайства. Електронне наукове видання «Аналітично-порівняльне правознавство». С.639-643 URL: <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/68788/1/303719-%d0%a2%d0%b5%d0%ba%d1%81%d1%82%20%d1%81%d1%82%d0%b0%d1%82%d1%82%d1%96-701625-1-10-20240510.pdf>

References

1. Bryskovska, O. M., Helemei, M. O. (2023). Osoblyvosti vchynennia shakhraistva v merezhi Internet v umovakh voiennoho stanu [Peculiarities of committing fraud on the Internet during martial law]. *Kyivskyi chasopys prava*, 3, 174-180. [in Ukrainian]
2. Karchevskiy, M. (2024). Protydiia zlochynnosti v Ukraini: infohrafika (2023-2024): intehraktyvnyi dovidnyk [Combating crime in Ukraine: infographics (2023-2024): interactive guide]. *CrimeDataLab*. Available at: <https://crimedatalab.org/> [in Ukrainian]
3. Usmanov, R. A. (2024). Deiaki pytannia ob'iektivnoi storony shakhraistva, vchynenoho shliakhom nezakonnykh operatsii z vykorystanniam EOT [Some issues of the objective side of fraud committed by illegal operations using electronic computing technology]. *Pravnychi chasopys Donetskoho natsionalnoho universytetu imeni Vasyilia Stusa*, (Ver), 223-229. DOI: <https://doi.org/10.31558/2786-5835.2024.1.22>. [in Ukrainian]
4. Usmanov, R. A. (2025). Kryminalna vidpovidalnist za shakhraistvo, vchynene shliakhom nezakonnykh operatsii iz vykorystanniam kompiuternoï tekhniki [Criminal liability for fraud committed by illegal operations using computer technology]. Ph.D. dissertation, DNUVS. Available at: <https://dnuvs.ukr.education/wp-content/uploads/2025/02/dysertac> [in Ukrainian]
5. Fortunova, M. H., Musiienko, A. V. (n.d.). Aktualni aspekty zapobihannia latentnii zlochynnosti [Actual aspects of preventing latent crime]. *Dictum Factum*, 283-306. Available at: <https://df.duit.in.ua/index.php/dictum/article/view/366> [in Ukrainian]
6. Chekmariova, I. M. (n.d.). Shakhraistvo v interneti yak odyn iz vydiv shakhraistva [Internet fraud as one of the types of fraud]. *Elektronne naukovye vydannia «Analitychno-porivnialne pravoznavstvo»*, 639-643. Available at: <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/68788/1/303719-%d0%a2%d0%b5%d0%ba%d1%81%d1%82%20%d1%81%d1%82%d0%b0%d1%82%d1%82%d1%96-701625-1-10-20240510.pdf>

%d0%a2%d0%b5%d0%ba%d1%81%d1%82%20%d1%81%d1%82%d0%b0%d1%82%d1%82%d1%96-701625-1-10-20240510.pdf [in Ukrainian]

PROBLEMS OF ACCOUNTING AND COUNTERACTING FRAUD IN THE CONTEXT OF MODERN CHALLENGES

Viktoriya Mykytiuk*, Oleksandra Ptashnyk**

* fourth-year student majoring in Law, King Danylo University (Ivano-Frankivsk, Ukraine)

**Acting Head of the Department of Law named after Acad. O.I.M. Lutsky, Candidate of Sociological Sciences, Associate Professor, King Danylo University (Ivano-Frankivsk, Ukraine)

The purpose of the study is to analyze the trends in the registration of criminal offenses on the grounds of fraud in Ukraine in 2024, to study and search for levers to regulate punishments for crimes committed, and to develop recommendations for improving the system of registration of offenses. The methodology includes a comprehensive analysis of the problem of fraud in modern conditions, especially in view of martial law and digitalization. The study is based on the analysis of official statistics for 2024, which demonstrates a paradoxical decrease in the number of registered proceedings, despite the complexity of fraud schemes. A comparative analysis of statistical data and scientific works of domestic researchers was used. It is established that the decrease in the number of recorded fraudulent offenses recorded in 2024 probably does not reflect a real improvement in the crime situation, but is a consequence of possible problems in keeping records of crimes, their registration and changes in methodology. It is found that modern forms of fraud actively use digital technologies, which complicates their detection, collection of evidence and prosecution. In particular, various types of online fraud, such as phishing messages, fake charity collections, and international aid fraud are considered. The author examines the difficulties in distinguishing between Articles 185 and 190 of the Criminal Code of Ukraine in the qualification of crimes committed with the use of computer technologies, which indicates the need for unification of law enforcement approach. Scientific novelty. The scientific novelty lies in the actualization of the problem of fraud latency in the context of the strengthening of its digital forms and martial law, as well as in the justification of the need for a systematic approach to counteracting this phenomenon. A set of measures is proposed, including the development of preventive monitoring using artificial intelligence, the creation of a unified register of cybercrime and the introduction of ethical hacking to identify and eliminate vulnerabilities in security systems. The results of the study can be used to improve the current legislation on the qualification of fraud in the context of digitalization, to develop effective strategies to combat cybercrime, and to raise public awareness of modern fraudulent schemes. The proposed recommendations will help improve the system of registration of offenses and ensure the principle of inevitability of punishment.

Key words: fraud, cybercrime, crime statistics, criminal law, phishing, ethical hacking, preventive monitoring, latent crime, bank fraud.

Дата першого надходження статті до видання: 20.10.2025
Дата прийняття статті до друку після рецензування: 20.11.2025
Дата публікації: 10.02.2026