



ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕКОНОМІЧНА БЕЗПЕКА

УДК 330.341.1

DOI: <https://doi.org/10.37332/2309-1533.2025.1.5>

JEL Classification: O30, O33, O36

Семенченко Н.В.,
д-р екон. наук, професор,
професор кафедри економічної кібернетики,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Мельничук В.Е.,
доктор філософії з економіки,
асистент кафедри економічної кібернетики,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Калініченко М.С.,
студентка групи KI-11 Інституту прикладного та системного аналізу,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

ВПЛИВ КРИПТОШАХРАЙСТВА НА ЦИФРОВУ ЕКОНОМІКУ: ЗРОСТАННЯ ВТРАТ ТА РОЛЬ КІБЕРБЕЗПЕКИ У МІНІМІЗАЦІЇ РИЗИКІВ

Semenchenko N.V.,
dr sc.(econ.), professor,
professor at the department of economic cybernetics,
National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”,
Melnychuk V.E.,
Ph.D. in Economics, assistant lecturer
at the department of economic cybernetics,
National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”,
Kalinichenko M.S.,
student of group KI-11 Institute for applied system analysis,
National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”

THE IMPACT OF CRYPTO FRAUD ON THE DIGITAL ECONOMY: INCREASE IN LOSSES AND THE ROLE OF CYBERSECURITY IN RISK MINIMIZATION

Постановка проблеми. Криптовалюти стали невід’ємною частиною сучасної цифрової економіки, відкриваючи нові можливості для фінансових операцій і децентралізованих рішень. Проте стрімке зростання популярності криптовалют супроводжується також збільшенням шахрайства. В умовах високої анонімності транзакцій і відсутності централізованого контролю, криптовалюти стали привабливими для зловмисників, що створює серйозні загрози для фінансової стабільності та безпеки користувачів. Однією з основних проблем є відсутність надійних механізмів захисту, які дозволяли б

мінімізувати ці ризики. У цьому контексті особливу роль відіграє розвиток і впровадження інноваційних технологій цифрової економіки для боротьби з криптошахрайством, зокрема використання штучного інтелекту для аналізу транзакцій та виявлення аномальної поведінки користувачів.

Аналіз останніх досліджень і публікацій. Останні дослідження у сфері криптовалют і криптошахрайства показують, що зростання інтересу до криптовалют супроводжується значним збільшенням шахрайських операцій, що має серйозні економічні наслідки для глобальних фінансових ринків. За даними різних звітів, у 2022 році загальні втрати від криптошахрайств склали \$3.8 мільярдів, що свідчить про високий рівень шахрайства у криптопросторі [8]. Криптовалюти, через свою децентралізовану природу та анонімність транзакцій, стали привабливими для зловмисників. На основі даних, наданих компанією Chainalysis, ринок криптовалют зазнає серйозних втрат через різноманітні шахрайські схеми, включаючи фішинг, скам, Ponzi-схеми та зломи гаманців [9].

Згідно з дослідженнями Forbes, криптошахрайство швидко зростає через відсутність достатнього регулювання та обмежену обізнаність користувачів щодо можливих шахрайських схем. Наприклад, дослідження CoinDesk вказує на те, що у 2021 році інвестори втратили \$3.1 мільярди через криптошахрайство, що є серйозною перешкодою для розвитку цього ринку [12]. Також, згідно з даними Statista, з 2011 по 2022 роки було зафіксовано значне збільшення втрат через злочини в криптовалютному секторі, що підкреслює необхідність посилення заходів безпеки для захисту цифрових активів [13].

Зважаючи на вищезгадані дослідження, окрему увагу варто приділити сучасним технологіям, таким як штучний інтелект (ШІ), для мінімізації криптошахрайства у цифровій економіці. Штучний інтелект може бути використаний для виявлення аномалій у транзакціях, що дозволяє здійснювати своєчасну ідентифікацію шахрайських дій. Наприклад, компанія iScutum вже розробляє системи на основі ШІ для покращення кібербезпеки в криптовалютному секторі [5].

Також велику роль у боротьбі з криптошахрайством відіграють інвестиції в навчання та підвищення обізнаності користувачів щодо методів захисту. Програми, які зосереджені на підвищенні обізнаності, можуть значно знизити кількість успішних атак. Наприклад, платформи для навчання кібербезпеці, такі як Awareness Training від iScutum, пропонують ліцензовані курси, які дозволяють користувачам краще розуміти потенційні загрози в цифровому середовищі [2, 7].

Оскільки більшість традиційних методів захисту недостатньо ефективні для криптовалютного ринку, особливо важливими є нові підходи, які включають інноваційні технічні рішення та міжнародне регулювання цифрової економіки, яке допоможе знизити ризики шахрайства та підвищити рівень безпеки цифрових активів.

Постановка завдання. Метою статті є дослідження впливу криптошахрайства на цифрову економіку, а також аналіз шляхів мінімізації ризиків шляхом впровадження інноваційних рішень у сфері кібербезпеки. У рамках дослідження розглядаються основні види шахрайства, його економічні наслідки, та пропонуються механізми, які допоможуть зменшити ризики шахрайства, зокрема за допомогою технологій штучного інтелекту.

Виклад основного матеріалу дослідження. Враховуючи відсутність централізованого регулювання та високу анонімність криптовалютних транзакцій, криптошахрайство стало однією з найсерйозніших проблем цифрової економіки. На ринку криптовалют зустрічається безліч видів шахрайства, кожен з яких має свої особливості та методи здійснення [6]. Одним із найпоширеніших видів криптошахрайства є фішинг, при якому шахраї використовують підроблені вебсайти, електронні листи або повідомлення для отримання конфіденційної інформації, такої як приватні ключі або логіни до криптовалютних гаманців [7]. Другим поширеним видом шахрайства є скам, що спрямований на залучення інвестицій або отримання доступу до чужих активів під виглядом легітимних криптопроектів. Атаки на гаманці, Ponzi-схеми, Rug Pull – ще декілька прикладів криптошахрайства, що стосуються виманювання коштів з гаманців. Оскільки криптовалютні транзакції є безповоротними, жертви таких атак, зазвичай, не можуть повернути свої кошти.

Однією з найбільш ризикових зон для шахрайства є первинні пропозиції монет (ICO), тобто процес залучення коштів на розвиток криптовалютного проекту шляхом продажу нових tokenів інвесторам [10]. Оскільки процес ICO є нерегульованим, часто трапляються випадки, коли шахраї створюють фальшиві ICO, обіцяючи високі прибутки та залучаючи великі суми інвестицій. Після збору коштів такі проекти можуть раптово зникати, залишаючи інвесторів без tokenів та капіталу.

Криптошахрайство має серйозний вплив на глобальну економіку, зокрема на інвестиційний клімат, довіру до криптовалют і фінансові ринки. Один з основних наслідків криптошахрайства – це зниження довіри інвесторів до криптовалютного ринку. Оскільки криптовалюти досі є відносно новим фінансовим інструментом цифрової економіки, кожен випадок шахрайства підриває віру інвесторів у безпеку та надійність цього ринку. Згідно зі статистикою [13], публікації у ЗМІ про великі шахрайства або крадіжки криптовалют часто призводять до різкого падіння вартості криптоактивів і зниження обсягів торгівлі. Кількість втрачених криптоактивів представлені на рис.1.

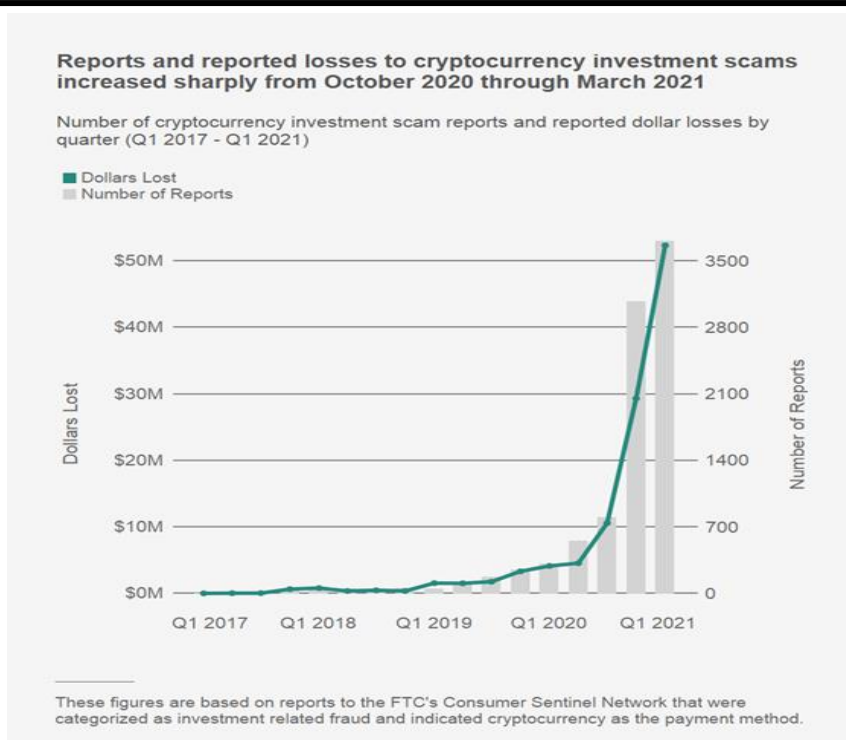


Рис. 1. Зростаюча тенденція кібератак з кількістю втрачених криптоактивів (в млн дол.)
Джерело: [13]

Крім того, вплив на інвестиційний клімат є особливо важливим у випадку нових технологій та інноваційних рішень, що базуються на блокчейні. Шахрайські дії у криптовалютній сфері стримують розвиток перспективних стартапів, адже потенційні інвестори бояться втратити свої активи через відсутність регуляторних механізмів захисту, що може сповільнити процес прийняття криптовалют і технології блокчейн на інституційному рівні [3; 8].

Фінансові ринки та регулюючі органи також страждають від наслідків криптошахрайства. Зростання кількості шахрайських операцій викликає необхідність посилення контролю з боку регуляторних органів. Наприклад, багато країн намагаються впровадити закони, що регулюють обіг криптовалют та боротьбу з відмиванням коштів у цифровій економіці. Однак через децентралізований характер криптовалют регулювання часто є складним і вимагає міжнародної координації. Уряди втрачають податкові надходження через нелегальні криптовалютні транзакції, а значні крадіжки криптоактивів призводять до втрати довіри до фінансових інструментів на основі блокчейну, що може уповільнити їх інтеграцію у світові ринки [9].

Загалом, тіньова економіка виграє від поширення криптошахрайства, оскільки анонімність криптовалют дозволяє зловмисникам уникати регуляторних органів і здійснювати нелегальні операції, що підриває стабільність світових фінансових ринків і створює нові виклики для регуляторів і урядів [12].

За останні роки обсяги вкрадених коштів у криптовалютному секторі значно зросли. Використовуючи фішинг, атаки на криптобіржі та злам смарт-контрактів, злочинці отримали доступ до мільярдних активів, що підкреслює необхідність нових рішень для захисту цифрових активів. Щорічне зростання масштабів шахрайства свідчить про те, що ця проблема стає дедалі актуальнішою і потребує негайного вирішення.

Сума збитків включає різні типи шахрайських схем, таких як крадіжки з криптогаманців, атаки на біржі, Ponzi-схеми та Rug Pull. Варто зазначити, що цей показник є значним кроком назад для ринку криптовалют, адже він підриває довіру інвесторів і стримує розвиток індустрії.

Протягом п'яти років кількість випадків шахрайства з використанням криптовалют стабільно зростала [13; 17]. Наприклад, у 2018 році втрати від криптошахрайства склали приблизно \$1,7 млрд, що на той момент було рекордним показником. У наступні роки кількість шахрайських операцій тільки зростала, досягнувши піку у 2022 році [17]. Кількість криптоатак з 2011 до 2024 року представлені на рис. 2. Важливим фактором цього зростання є зростання популярності децентралізованих фінансів (DeFi) та ICO, які часто стають мішенню для шахраїв через недостатність регуляторного контролю.

Crypto hacks & scams per year by number from 2011 to March 6, 2024

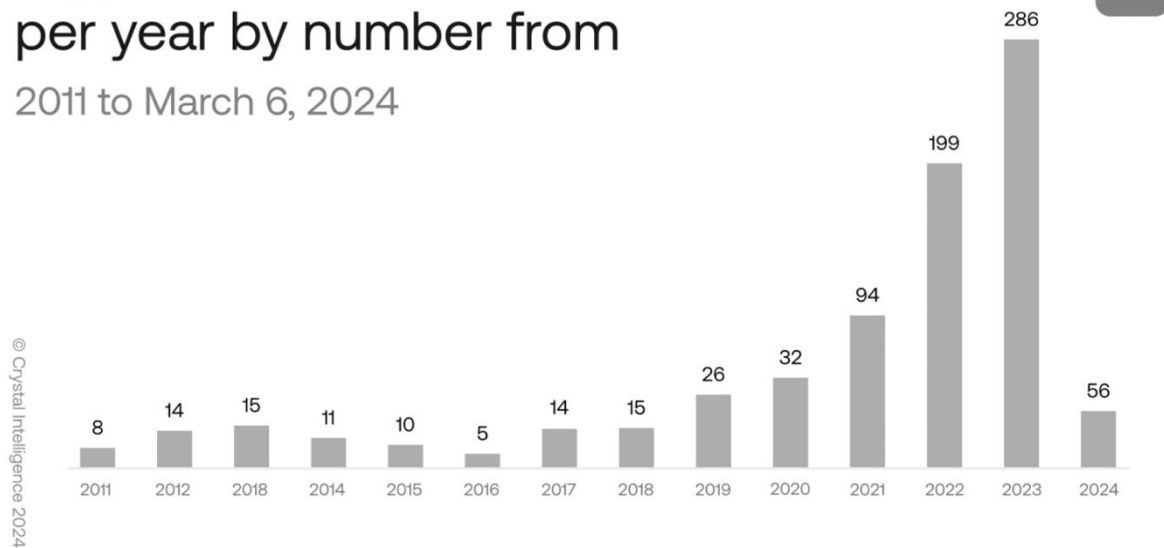


Рис. 2. Тенденція зростаючої кількості кібератак та шахрайства

Джерело: [19]

За оцінками фінансових експертів, втрати від традиційних банківських шахрайств, таких як фальшиві транзакції та крадіжки з кредитних карток, складають приблизно \$4–6 млрд щорічно [10; 13]. Проте варто враховувати, що традиційні фінансові системи мають набагато більш розвинені механізми захисту та регулювання, тоді як криптовалюти ще не отримали достатньої уваги з боку державних органів. Не варто скидати з рахунків і численні кібератаки від російських хакерів на українську банківську систему [1; 4], критичну інфраструктуру [16] та держсектор з метою заволодіння особистими даними українців та скоєння зловмисних дій.

Динаміка зростання криптозлочинів з 2015 по 2023 роки демонструє значну ескалацію [13]. З 2015 року, коли ринок криптовалют лише починав набирати обертів, кількість шахрайських випадків була відносно невеликою. Проте вже з 2017 року, після різкого зростання вартості біткоїна та інших криптовалют, шахраї почали активно використовувати нові можливості для незаконного збагачення [15].

Одним із найбільш відомих випадків криптошахрайства є злом криптобіржі Mt. Gox, який стався у 2014 році, коли було втрачено понад 850 тисяч біткоїнів (що на той момент оцінювалося у понад \$450 млн). Цей інцидент викликав серйозний резонанс у світі криптовалют і став поштовхом до розвитку нових методів захисту, хоча подібні зломи повторювалися у наступні роки [11; 12].

Наприклад, у 2022 році з криптобіржі FTX було викрадено понад \$600 млн, що стало ще одним гучним скандалом у світі криптовалют [18]. Ці атаки демонструють, що навіть великі та популярні біржі не можуть повністю захистити себе від шахраїв, що знижує довіру інвесторів і викликає необхідність у жорсткішому регулюванні галузі.

Особливу увагу привертає вплив децентралізованих фінансів (DeFi) на зростання кількості шахрайських операцій. DeFi-платформи пропонують можливість користувачам здійснювати фінансові операції без участі посередників, таких як банки або брокери, використовуючи смарт-контракти. Проте відсутність централізованого контролю робить ці платформи вразливими для шахраїв. Згідно зі статистикою Chainalysis [9], у 2021 році понад 40 % втрат у криптовалютах припадало саме на Rug Pull, що свідчить про необхідність посилення регуляторного нагляду та захисту інвесторів на платформах DeFi.

Криптошахрайство чинить значний вплив на економічну ефективність ринку. В основі лежить модель витрат і втрат, яка демонструє, як шахрайські операції створюють негативні зовнішні ефекти [9]. Учасники ринку, зокрема інвестори та компанії, зазнають прямих фінансових збитків через крадіжки активів. Крім того, втрата довіри до криптовалютної інфраструктури призводить до втраченої вигоди, що знижує загальну ефективність ринку криптовалют, що впливає на економічну інфраструктуру. Шахрайства підривають можливості для інновацій, оскільки стартапи та компанії з обмеженими фінансовими ресурсами не можуть розвиватися в умовах високих ризиків. Відповідно, криптовалютні шахрайства створюють перешкоди для розвитку технологій блокчейн і DeFi, уповільнюючи прогрес і економічні перспективи для нових учасників ринку.

Зростання криптовалютного ринку призвело до появи нових загроз у вигляді криптошахрайства. Кібербезпекові компанії розробляють різноманітні інструменти, що допомагають забезпечити безпеку криптоактивів для зниження ризиків втрат та захисту активів, серед яких є використання штучного інтелекту для виявлення аномальної поведінки користувачів. Тобто, системи ШІ можуть аналізувати великі масиви поведінкових даних, таких як рухи миші, швидкість набору тексту, частоту кліків тощо. Завдяки машинному навчанню, ШІ виявляє нетипову активність, що може свідчити про несанкціонований доступ до криптогаманця або біржі, що дозволяє оперативно вживати заходів для захисту активів.

Мультифакторна автентифікація (MFA) також є важливим інструментом захисту, що забезпечує додатковий рівень безпеки і значно ускладнює несанкціонований доступ до криптоактивів, навіть якщо зломисники отримали доступ до пароля. Крім того, криптографічні методи є невід'ємною частиною захисту криптовалютних гаманців. Шифрування приватних ключів забезпечує захист від компрометації та несанкціонованого використання. Використання складних криптографічних алгоритмів унеможливорює несанкціонований доступ до коштів у разі зламу або крадіжки пристрою. Проте, найбільш перспективний підхід до захисту криптовалютного ринку – це інтеграція штучного інтелекту. Наприклад, стартап, який створюється при підтримці кібербезпекової компанії iScutum [5], розробляє платформу на основі ШІ, яка аналізує поведінку користувачів у реальному часі для виявлення потенційних загроз. Завдяки використанню машинного навчання, платформа може розпізнавати навіть найменші зміни у поведінці, що дозволяє зменшити кількість помилкових тривог і підвищити ефективність виявлення загроз. ШІ здатний швидко адаптуватися до нових типів шахрайств, що робить його ключовим інструментом у боротьбі з криптошахрайством. Платформа також інтегрує додаткові рівні безпеки, наприклад, автоматичне включення мультифакторної автентифікації або блокування доступу до акаунту у разі виявлення підозрілої активності. Це дозволяє оперативно реагувати на можливі атаки, знижуючи ризики втрат активів.

При постійно зростаючому ризику криптошахрайств важливо не лише використовувати існуючі методи захисту, а й розробляти нові технології для підвищення безпеки криптовалютних платформ [16]. Наприклад, використання блокчейн-протоколів безпеки, які базуються на децентралізованій природі блокчейну та можуть забезпечити високий рівень безпеки, мають можливість мінімізувати централізовані атаки на біржі та гаманці. Інтеграція штучного інтелекту у криптовалютні платформи є ще одним перспективним напрямом. Використання ШІ для постійного моніторингу та аналізу транзакцій дозволить виявляти шахрайські схеми ще на ранніх етапах, суттєво знижуючи ризики для інвесторів і забезпечуючи високий рівень довіри до криптовалютного ринку.

Безперечно, у майбутньому можна очікувати появу нових інноваційних рішень [5] для забезпечення безпеки криптовалютних активів, що базуватимуться на синергії штучного інтелекту та криптографічних методів.

Сучасний стан ринку криптовалют характеризується значним ризиком шахрайства через відсутність чіткої регуляторної бази. Для мінімізації криптошахрайства важливо впровадити державне регулювання, яке забезпечить вищу прозорість і довіру до криптовалютних операцій. Наприклад, встановлення обов'язкових стандартів для криптовалютних бірж і платформ, що дозволить зменшити можливості для шахраїв. Крім того, слід розглянути створення глобальних регулюючих органів для контролю за криптовалютними операціями, які координуватимуть дії між країнами, розроблятимуть спільні стратегії і правила, які допоможуть боротися з міжнародними криптошахрайствами. Наприклад, міжнародні угоди про спільну відповідальність можуть спростити процедури переслідування шахраїв і покращити обмін інформацією між правоохоронними органами різних країн.

Окрім цього, важливим аспектом мінімізації криптошахрайства є впровадження технологічних інновацій. Наприклад, захищені апаратні гаманці є надійним способом зберігання криптовалют, оскільки вони зберігають приватні ключі в безпечному середовищі, недоступному для інтернет-атак, що зменшують ризики зламу та крадіжки активів. Також необхідно запровадити безпечні алгоритми смарт-контрактів, використання яких дозволить автоматизувати процеси, пов'язані з транзакціями, та зменшити можливості для шахрайських дій. Наприклад, розробка стандартів для перевірки коду смарт-контрактів перед їх використанням може допомогти виявити уразливості, які можуть бути використані шахраями.

Останнім, але не менш важливим аспектом мінімізації криптошахрайства у цифровій економіці є реалізація стратегій підвищення обізнаності серед користувачів. Освітні програми грають важливу роль у формуванні свідомості про ризики, пов'язані з криптовалютами, а також про методи шахрайства і засоби захисту від них. Інформування користувачів про основні види шахрайств, такі як фішинг, скам або Ponzi-схеми, дозволить зменшити кількість жертв криптошахрайства.

У цьому контексті компанія iScutum пропонує програму Learning Awareness Training, яка надає ліцензовані курси з кібербезпеки в Україні [2]. Ці програми зосереджені на навчанні користувачів методам захисту та виявлення шахрайських схем, що сприяє підвищенню їхньої обізнаності та зменшенню ризиків. Освіта та інформаційні кампанії можуть суттєво поліпшити розуміння користувачами важливості кібербезпеки та впровадження заходів захисту.

Висновки з проведеного дослідження. У процесі проведеного дослідження було виявлено, що криптошахрайство становить серйозну загрозу для фінансової стабільності, інвестиційного клімату та довіри до криптовалют. Основні результати дослідження підтверджують, що масштаби криптошахрайства за останні роки значно зросли, причому втрачені кошти перевищують мільярди доларів. Злочинці використовують різноманітні схеми, включаючи фішинг, Ponzi-схеми, атаки на гаманці та інші шахрайські методи, що вимагає термінових заходів для захисту інвесторів та стабільності ринку.

Важливість розвитку штучного інтелекту у боротьбі з криптошахрайством не можна переоцінити. ШІ має потенціал для автоматизації процесів виявлення шахрайських дій, аналізуючи величезні обсяги даних в реальному часі. Використання алгоритмів машинного навчання для виявлення аномальної поведінки користувачів може значно підвищити рівень безпеки криптовалютних платформ. Розробка систем на основі ШІ, здатних адаптуватися до нових шахрайських методів, дозволить не лише виявляти загрози, але й прогнозувати потенційні атаки, забезпечуючи проактивний підхід до кібербезпеки.

На основі проведеного аналізу можна сформулювати ряд рекомендацій для регулюючих органів, урядів і бізнесу, що стосуються регулювання та законодавства, а саме розроблення чітких регуляторних рамок, які забезпечать прозорість та підзвітність на ринку криптовалют. Важливо запровадити стандарти для криптобірж та платформ, а також створити міжнародні угоди для боротьби з транснаціональними криптошахрайствами. Наступним кроком може стати підтримка технологій безпеки: інвестиції в новітні технології, такі як рішення на базі ШІ для виявлення шахрайства, можуть суттєво поліпшити рівень безпеки, а блокчейн-протоколи безпеки повинні стати невід'ємною частиною стратегій протидії шахрайству. На наш погляд, освіта та підвищення обізнаності, а саме впровадження програм, таких як Learning Awareness Training від iScutum, допоможуть підвищити рівень знань про методи шахрайства та захисту від них. Співпраця з кібербезпековими компаніями, взаємодія між урядами, та регуляторними органами може призвести до ефективніших стратегій боротьби з шахрайством, не лише в розробці нових рішень, а й у швидкому реагуванні на виникаючі загрози. Нарешті, цифрова економіка, а саме технології передачі грошей повинні бути фінансово прозорими. Уряди повинні запроваджувати механізми, що забезпечують фінансову прозорість, у тому числі у сфері криптовалют, включаючи обов'язкову звітність для учасників ринку і вдосконалення механізмів контролю за транзакціями. Таким чином, комплексний підхід до боротьби з криптошахрайством, що включає регуляцію, технології безпеки та освітні програми, дозволить не лише знизити ризики, а й сприяти розвитку надійного та безпечного ринку криптовалют та цифрової економіки в цілому.

Література

1. Криптошахрайство: вплив на ринок та економічні наслідки. *OGoMono*. 2024. URL: <https://t.me/OGoMono/1826> (дата звернення: 24.01.2025).
2. Навчання обізнаності. *iScutum*. 2024. URL: <https://iscutum.com/uk/awareness-training> (дата звернення: 22.01.2025).
3. Найбільші криптошахрайства 2021 року. *CoinTelegraph*. 2021. URL: <https://cointelegraph.com/news/the-biggest-crypto-scams-of-2021> (дата звернення: 10.01.2025).
4. Ресурси для вивчення. *YuraGnatyuk*. 2024. URL: <https://t.me/yuragnatyuk/318> (дата звернення: 28.01.2025).
5. Рішення. *iScutum*. 2024. URL: <https://iscutum.com/uk/solutions> (дата звернення: 25.01.2025).
6. Топ-5 схем криптошахрайства. *FinTech Insider*. 2024. URL: <https://fintechinsider.com.ua/top-5-shem-kryptoshahrajstva-yak-zahystytys-vid-aferystiv> (дата звернення: 12.01.2025).
7. Управління вразливістю. *iScutum*. 2024. URL: <https://iscutum.com/uk/vulnerability-management> (дата звернення: 20.01.2025).
8. 3 billion lost to crypto scams in 2022. *The Block*. 2022. URL: <https://www.theblock.co/post/197183/3-billion-lost-to-crypto-scams-in-2022> (дата звернення: 25.01.2025).
9. Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity. *Chainalysis*. 2022. URL: <https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction> (дата звернення: 15.01.2025).
10. Cryptocurrency crime and anti money laundering report. *CipherTrace*. 2022. URL: <https://ciphertrace.com/2022-cryptocurrency-crime-and-anti-money-laundering-report> (дата звернення: 22.01.2025).
11. Cryptocurrency scams surged 2021 FTC says. *Reuters*. 2021. URL: <https://www.reuters.com/legal/cryptocurrency-scams-surged-2021-ftc-says-2022-01-27> (дата звернення: 12.01.2025).
12. Cryptoscams cost investors 31 billion in 2021. *CoinDesk*. 2022. URL: <https://www.coindesk.com/policy/2022/01/25/crypto-scams-cost-investors-31-billion-in-2021> (дата звернення: 18.01.2025).

13. Global cryptocurrency losses due to hacks and scams. *Statista*. 2022. URL: <https://www.statista.com/statistics/1291516/global-cryptocurrency-losses-due-to-hacks-and-scams> (дата звернення: 20.01.2025).
14. How crypto scams work and how to avoid them. *Business Insider*. 2024. URL: <https://markets.businessinsider.com/news/currencies/how-crypto-scams-work-and-how-to-avoid-them-1028376575> (дата звернення: 28.01.2025).
15. Increasing of fraud in cryptocurrency sphere. *Financial Times*. 2021. URL: <https://www.ft.com/content/e6486450-11ea-11ec-9d0e-1b28b8c36a40> (дата звернення: 30.01.2025).
16. Mundlamuri R., Midhunchakkaravarthy, D., Dandu, S. Joint detection and classification of signature and NetFlow based internet worms using MBGWO-based hybrid LSTM. *Journal of Computer Virology and Hacking Techniques*. 2022. 19. URL: <https://www.researchgate.net/publication/362614366> (дата звернення: 18.01.2025).
17. The growth of cryptocurrency fraud. *Forbes*. 2021. URL: <https://www.forbes.com/sites/bernardmarr/2021/08/16/the-growth-of-cryptocurrency-fraud> (дата звернення: 08.01.2025).
18. The state of the cryptocurrency market. *McKinsey & Company*. 2021. URL: <https://www.mckinsey.com/industries/financial-services/our-insights/the-state-of-the-cryptocurrency-market> (дата звернення: 05.01.2025).
19. Thirteen years of crypto crimes unveiled. *Crystal Intelligence*. 2024. URL: <https://crystalintelligence.com/investigations/thirteen-years-of-crypto-crimes-unveiled> (дата звернення: 15.01.2025).

References

1. OGoMono (2024), Cryptofraud: Market Impact and Economic Consequences, available at: <https://t.me/OGoMono/1826> (access date January 24, 2025).
2. iScutum (2024), Awareness training, available at: <https://iscutum.com/uk/awareness-training> (access date January 22, 2025).
3. CoinTelegraph (2021), The biggest crypto scams in 2021, available at: <https://cointelegraph.com/news/the-biggest-crypto-scams-of-2021> (access date January 10, 2025).
4. YuraGnatyuk (2024), Resources for study, available at: <https://t.me/yuragnatyuk/318> (access date January 28, 2025).
5. iScutum (2024), Solutions, available at: <https://iscutum.com/uk/solutions> (access date January 25, 2025).
6. FinTech Insider (2024), Top 5 crypto fraud schemes, available at: <https://fintechinsider.com.ua/top-5-shem-kryptoshahrajstva-yak-zahystytys-vid-aferystiv> (access date January 12, 2025).
7. iScutum (2024), Vulnerability management, available at: <https://iscutum.com/uk/vulnerability-management> (access date January 20, 2025).
8. The Block (2022), \$3 billion lost to crypto scams in 2022, available at: <https://www.theblock.co/post/197183/3-billion-lost-to-crypto-scams-in-2022> (access date January 25, 2025).
9. Chainalysis (2022), Crypto crime report 2022, available at: <https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction> (access date January 15, 2025).
10. CipherTrace (2022), 2022 cryptocurrency crime and anti-money laundering report, available at: <https://ciphertrace.com/2022-cryptocurrency-crime-and-anti-money-laundering-report> (access date January 22, 2025).
11. Reuters (2021), Cryptocurrency scams surged in 2021, FTC says, available at: <https://www.reuters.com/legal/cryptocurrency-scams-surged-2021-ftc-says-2022-01-27> (access date January 12, 2025).
12. CoinDesk (2022), Crypto scams cost investors \$3.1 billion in 2021, available at: <https://www.coindesk.com/policy/2022/01/25/crypto-scams-cost-investors-31-billion-in-2021> (access date January 18, 2025).
13. Statista (2022), Value of cryptocurrency losses due to hacks and scams worldwide from 2011 to 2022, available at: <https://www.statista.com/statistics/1291516/global-cryptocurrency-losses-due-to-hacks-and-scams> (access date January 20, 2025).
14. Business Insider (2024), How crypto scams work and how to avoid them, available at: <https://markets.businessinsider.com/news/currencies/how-crypto-scams-work-and-how-to-avoid-them-1028376575> (access date January 28, 2025).
15. Financial Times (2021), The rise of cryptocurrency crime, available at: <https://www.ft.com/content/e6486450-11ea-11ec-9d0e-1b28b8c36a40> (access date January 30, 2025).
16. Rao, Mundlamuri & Midhunchakkaravarthy, Divya & Dandu, Sujatha. (2022), Joint detection and classification of signature and NetFlow based internet worms using MBGWO-based hybrid LSTM. *Journal of Computer Virology and Hacking Techniques*. 19, available at: <https://www.researchgate.net/publication/362614366> (access date January 18, 2025).

17. Forbes (2021), The growth of cryptocurrency fraud, available at: <https://www.forbes.com/sites/bernardmarr/2021/08/16/the-growth-of-cryptocurrency-fraud> (access date January 8, 2025).

18. McKinsey & Company (2021), The state of the cryptocurrency market, available at: <https://www.mckinsey.com/industries/financial-services/our-insights/the-state-of-the-cryptocurrency-market> (access date January 5, 2025).

19. Crystal Intelligence (2024), Thirteen years of crypto crimes unveiled, available at: <https://crystalintelligence.com/investigations/thirteen-years-of-crypto-crimes-unveiled> (access date January 15, 2025).

Семенченко Н.В., Мельничук В.Е., Калініченко М.С.

ВПЛИВ КРИПТОШАХРАЙСТВА НА ЦИФРОВУ ЕКОНОМІКУ: ЗРОСТАННЯ ВТРАТ ТА РОЛЬ КІБЕРБЕЗПЕКИ У МІНІМІЗАЦІЇ РИЗИКІВ

Мета. Дослідження впливу криптошахрайства на цифрову економіку, а також аналіз шляхів мінімізації ризиків шляхом впровадження інноваційних рішень у сфері кібербезпеки.

Методика дослідження. Дослідження використовує комбінацію аналітичних та емпіричних методів для вивчення впливу криптошахрайства на цифрову економіку. Дані з авторитетних фінансових джерел і джерел кібербезпеки, таких як Chainalysis, CoinDesk і Forbes, використовуються для оцінки фінансових втрат, спричинених шахрайством. Статистичний аналіз використовується для вивчення тенденцій шахрайства з криптовалютою за останні роки.

Результати дослідження. Розглянуто типи криптошахрайства, такі як фішинг, ринкові маніпуляції, інвестиційні шахрайські схеми та зломи гаманців. Виявлено, що ці дії призводять до значних фінансових втрат, зниження довіри до цифрових активів та дестабілізації інвестиційного клімату. Проаналізовано інноваційні підходи до мінімізації ризиків, зокрема використання штучного інтелекту для аналізу транзакцій і поведінкових патернів користувачів. Виявлено, що системи, засновані на технологіях машинного навчання, дозволяють виявляти аномальні дії в режимі реального часу та активувати додаткові заходи захисту, що сприяє підвищенню безпеки у криптовалютній сфері. Запропоновано рішення, спрямовані на зниження економічних збитків та захист інвесторів, що підвищує довіру до криптовалютних технологій. Використання штучного інтелекту дозволяє ефективніше боротися з криптошахрайством і забезпечувати стабільність ринку цифрових активів.

Наукова новизна результатів дослідження. Вперше обґрунтовано економічних наслідків криптошахрайства, наголошуючи на необхідності заходів кібербезпеки, керованих ШІ. Встановлено, що використання багаторівневої стратегії, яка поєднує регуляторну політику, технологічний прогрес та інформаційні кампанії сприятиме зменшенню ризиків у сфері криптоактивів. Доведено ключову роль штучного інтелекту у виявленні шахрайських дій і зміцненні довіри до екосистеми криптовалют.

Практична значущість результатів дослідження. Результати дослідження мають значну практичну цінність для регуляторних органів, фінансових установ, інвесторів та розробників технологій кібербезпеки. Запропоновані заходи щодо мінімізації криптошахрайства можуть бути використані для вдосконалення нормативно-правової бази у сфері цифрової економіки та криптовалютного регулювання. Також практична значущість дослідження полягає у формуванні рекомендацій для бізнесу та криптобірж щодо впровадження передових технологічних рішень у сфері безпеки. Виявлені закономірності зростання шахрайства можуть допомогти розробити стратегії захисту інвесторів та забезпечення фінансової стабільності криптовалютного ринку.

Ключові слова: криптовалюта, шахрайство, штучний інтелект, економічна безпека, цифрова економіка.

Semenchenko N.V., Melnychuk V.E., Kalinichenko M.S.

THE IMPACT OF CRYPTO FRAUD ON THE DIGITAL ECONOMY: INCREASE IN LOSSES AND THE ROLE OF CYBERSECURITY IN RISK MINIMIZATION

Purpose. The aim of this article is to study the impact of crypto fraud on the digital economy, as well as to analyse ways to minimize risks by implementing innovative cybersecurity solutions.

Methodology of research. The study uses a combination of analytical and empirical methods to study the impact of crypto fraud on the digital economy. Data from reputable financial and cybersecurity sources such as Chainalysis, CoinDesk, and Forbes are created to estimate financial losses caused by fraud. Statistical analysis is used to study cryptocurrency fraud trends over the past years.

Findings. Types of crypto fraud are considered, such as phishing, market manipulation, investment fraud schemes, and wallet hacking. It is found that these actions lead to significant financial losses, reduce trust in digital assets, and destabilize the investment climate. Innovative approaches to minimizing risks are analysed, including using artificial intelligence to analyse transactions and behavioural patterns of users. It is found that systems based on machine learning technologies allow the detection of anomalous actions in real time and activate additional protection measures, which increases security in the cryptocurrency sector. Solutions aimed at reducing economic losses and protecting investors are proposed, which increases

confidence in cryptocurrency technologies. Artificial intelligence allows for more effective combat against crypto fraud and ensures the stability of the digital asset market.

Originality. The economic impact of crypto fraud is substantiated for the first time, highlighting the need for AI-driven cybersecurity measures. It is established that the use of a multi-layered strategy that combines regulatory policy, technological progress and information campaigns will help reduce risks in the crypto-asset sector. The key role of artificial intelligence in detecting fraudulent activities and strengthening trust in the cryptocurrency ecosystem is proven.

Practical value. The study results have significant practical value for regulatory authorities, financial institutions, investors and developers of cybersecurity technologies. The proposed measures to minimize crypto fraud can be used to improve the regulatory and legal framework in the digital economy and cryptocurrency regulation. Also, the practical significance of the study is impossible in forming recommendations for business and crypto exchanges on the implementation of advanced technological solutions in the security field. The revealed patterns of fraud growth can help develop strategies to protect investors and ensure the financial stability of the cryptocurrency market.

Key words: cryptocurrency, fraud, artificial intelligence, economic security, digital economy.