Аналітика ризиків втрати цифрових активів упродовж життєвого циклу власника

Закаблуківський Артем Валерійович [1]

Опубліковано	Секція	УДК
27.10.2025	Соціальні та поведінкові науки	004.056.5:336.74

DOI: https://doi.org/10.5281/zenodo.17457634

Анотація. Актуальність дослідження зумовлена зростанням кількості випадків, пов'язаних із втратою, несанкціонованим доступом або знищенням цифрових активів, зокрема криптовалют, токенів і персональних даних, що становить значні економічні й репутаційні загрози для окремих осіб та інституцій. Мета статті – дослідити ризики втрати цифрових активів на різних етапах їхнього життєвого циклу – від формування і зберігання до використання, передання й утилізації – та окреслити аналітичні підходи, що дають змогу за допомогою технологічних, організаційних і правових інструментів мінімізувати ці ризики. Результати дослідження показують, що кожен етап життєвого циклу активу створює специфічні конфігурації загроз. Висновки свідчать, що ефективний захист цифрових активів вимагає постійного моніторингу й адаптивного управління, а не ізольованих запобіжних заходів. Розвиток цифрової грамотності, впровадження багаторівневих систем автентифікації та шифрування, а також застосування правових інструментів, таких як цифрові заповіти й контракти про управління активами, формують основу стійкої цифрової власності.

Ключові слова: управління ризиками, цифрова безпека, захист даних, криптоактиви, блокчейн, правове регулювання.

Analytics of risks of loss of digital assets throughout the owner's lifecycle

Annotation. The growing integration of digital assets into economic and social systems underscores the importance of developing comprehensive mechanisms for their protection throughout their entire life cycle. The relevance of the study is determined by the rising number of cases related to the loss, unauthorized access, or destruction of digital assets, including cryptocurrencies, tokens, and personal data, which pose significant economic and reputational threats to individuals and institutions. The purpose of the article is to analyze the risks of losing digital assets at different stages of their life cycle — from creation and storage to use, transfer, and disposal – and to identify analytical approaches that enable the minimization of these risks through technological, organizational, and legal tools.

The research results show that each stage of the asset life cycle generates specific configurations of threats. At the formation stage, the main risks arise from design flaws, insufficient verification, and fraudulent issuance of digital assets. During the storage and administration stage, dominant factors include technical vulnerabilities, loss of cryptographic keys, and breaches of access protocols. The use and circulation stage is associated with market

[1] менеджер проєктів, «NOTA Дослідницький центр цифрових валют», м. Сакраменто, США, M0957300684@gmail.com, ORCID: https://orcid.org/0009-0005-9167-5728

volatility, transactional errors, and social engineering attacks that exploit human behavior. The transfer and inheritance stage is characterized by legal and procedural uncertainty, particularly concerning ownership succession and cross-border jurisdiction. In the final stage, related to disposal or obsolescence, threats arise from improper data destruction and the potential recovery of confidential information. The study emphasizes the need for an integrated risk assessment system that combines cybersecurity analytics, probabilistic modeling, and behavioral economics to determine the likelihood and potential impact of data loss events.

The conclusions indicate that adequate digital asset protection requires continuous monitoring and adaptive management rather than isolated preventive measures. The development of digital literacy, implementation of multi-level authentication and encryption systems, and the use of legal tools such as digital wills and asset management contracts form the foundation of sustainable digital ownership. The study also highlights the growing role of artificial intelligence and big data in predictive risk analytics, which ensures early anomaly detection and proactive protection. The results demonstrate that establishing a coordinated digital asset risk management system at the individual, institutional, and state levels can ensure long-term stability, transparency, and trust in the digital economy.

Keywords: risk management, digital security, data protection, crypto-assets, blockchain, legal regulation.

Вступ

Швидка диджиталізація світової економіки перетворила цифрові активи на ключовий компонент сучасних фінансових та інформаційних систем. Криптовалюти, токени, невзаємозамінні активи і цифрові гаманці дедалі частіше стають не лише інструментами обміну та інвестування, але й носіями особистої та корпоративної цінності. Але технологічна й правова інфраструктура, що їх підтримує, залишається вкрай розрізненою та вразливою. Вирішення проблеми втрати цифрових активів – чи то через несанкціонований доступ, чи то внаслідок пошкодження даних, чи то через неправильне управління ключами, чи то з огляду на юридичну невизначеність – стало одним із найважливіших завдань цифрової економіки. Відсутність стандартизованих механізмів виявлення, оцінювання та зменшення ризиків зумовлює для власників виникнення комплексних небезпек, що поєднують технічні несправності, людські помилки й економічну нестабільність. Така велика кількість ризиків вимагає системного аналітичного підходу, здатного відстежувати їх у динаміці протягом усього життєвого циклу володіння активами – від створення та зберігання до обігу, передання й остаточної утилізації.

Актуальність вивчення аналітики ризиків втрати цифрових активів зумовлена необхідністю подолання невідповідності між технологічними інноваціями та механізмами захисту й регулювання, що їх супроводжують. У процесі накопичення цифровими активами реальної економічної ваги їхня безпека безпосередньо пов'язується з фінансовою стабільністю, довірою інвесторів і збереженням суверенітету даних. Традиційні методології управління ризиками є непридатними для врахування децентралізованої, транскордонної та алгоритмічно керованої природи цифрових середовищ. Тому необхідна нова аналітична парадигма, яка би поєднувала кібербезпеку, поведінкову економіку та правове управління для прогнозування, оцінювання й мінімізації ризиків на кожному етапі існування активу. Вивчення цього питання не лише сприяє теоретичному розвитку цифрової економіки, але й має практичне значення для сталого та безпечного функціонування екосистеми цифрових активів.

Аналіз сучасних досліджень і публікацій свідчить про зростання наукового інтересу до проблем управління ризиками у сфері цифрових активів, їхньої безпеки та правового регулювання. У роботі О. Коростіна [1] досліджено можливості застосування штучного інтелекту для оптимізації логістичних процесів, що демонструє потенціал

аналітичних технологій для підвищення ефективності управління ризиками в цифровому середовищі, що є однією зі сторін проблематики, яку розглянуто в статті. І. М. Гонак [2] аналізує проблеми функціонування криптовалютного бізнесу, виокремлюючи такі загрози, як волатильність ринку, кіберзлочинність і недосконалість нормативно-правової бази, що створює підґрунтя для подальших досліджень ризиків втрати цифрових активів. С. В. Волосович іта І. І. Нападовський [3] зосереджують увагу на специфіці ризиків, пов'язаних із криптовалютними активами, та механізмах їх страхування, наголошуючи на необхідності створення фінансових інструментів для зниження потенційних втрат користувачів.

Б. Ю. Москвін [4] аналізує перспективи розвитку правового регулювання цифрових активів в Україні, окреслюючи проблеми гармонізації національного законодавства з європейськими стандартами, що є важливим аспектом зниження правових ризиків у процесі володіння цифровими ресурсами та їх обігу. М. Левченко [5] розглядає маркетингові стратегії бізнес-розвитку на нових ринках із використанням цифрових інструментів, підкреслюючи значення аналітики даних і цифрових активів у формуванні конкурентних переваг, що опосередковано впливає на систему ризик-менеджменту. М. Зінченко, О. Мостовенко та І. Корсун [6] досліджують переваги й ризики цифрових грошей для економіки, акцентуючи зростання кіберзагроз та необхідність розвитку інфраструктури для захисту фінансових даних у цифровому просторі. Є. М. Мехович [7] у своїй роботі розглядає питання інтеграції цифрових фінансових активів у платіжну систему, пропонуючи прогнозні підходи до запобігання ризикам і формування стійкої системи цифрових розрахунків, що має безпосереднє значення для управління ризиками втрати активів упродовж життєвого циклу.

Мета статті – аналіз ризиків втрати цифрових активів на різних етапах їхнього життєвого циклу – від формування та зберігання до використання, передання й утилізації – та окреслення аналітичних підходів, що дають змогу за допомогою технологічних, організаційних і правових інструментів мінімізувати ці ризики.

Відповідно до мети перед нами були поставлені такі завдання: визначити класифікацію основних ризиків втрати цифрових активів на різних етапах їхнього життєвого циклу; проаналізувати технологічні, організаційні та правові чинники, що впливають на рівень цих ризиків; розробити аналітичну модель оцінювання й моніторингу ризиків втрати цифрових активів; обґрунтувати практичні підходи до їх мінімізації в сучасному цифровому середовищі.

Результати

Теоретичні та методологічні засади аналізу ризиків втрати цифрових активів базуються на вивченні природи, класифікації та економічної цінності цифрових активів, а також механізмів, що визначають їхню вразливість у цифровому середовищі. Цифровий актив є формою цінності, що існує виключно в електронному вигляді та залежить від цифрової інфраструктури для створення, зберігання, передання й використання. Це поняття охоплює широкий спектр елементів, зокрема криптовалюти, які функціонують як децентралізовані засоби обміну або інвестиційні інструменти; токени, що представляють цифрові права на матеріальні чи нематеріальні активи; невзаємозамінні токени (NFT), які уособлюють різні унікальні цифрові об'єкти, такі як твори мистецтва або предмети колекціонування; цифрові дані та онлайн-акаунти, що виконують функцію сховищ особистої, фінансової або корпоративної інформації. Кожна категорія цифрових активів має специфічні характеристики права власності, можливості передання й безпеки, що визначає різні типи ризиків та аналітичні напрями їх оцінювання.

У галузі цифрової безпеки поняття ризику визначається як імовірність настання несприятливої події, що призводить до часткової або повної втрати цифрового активу

або контролю над ним [8, с. 375]. На відміну від традиційних форм власності, втрата цифрового активу може проявлятися кількома різними способами. Одна з найважливіших особливостей полягає у відмінності між втратою доступу та втратою активу. Втрата доступу відбувається тоді, коли сам актив продовжує існувати в мережі або блокчейні, але законний власник не може здійснювати контроль через втрату криптографічних ключів, скомпрометовані паролі чи системні збої. Цей тип ризику найбільш актуальний для децентралізованих систем, де жодна центральна інстанція не може відновити доступ. Руйнування активу, навпаки, означає незворотне зникнення або пошкодження цифрового об'єкта чи запису через навмисні кібератаки, шкідливе програмне забезпечення або деградацію даних. Обидві форми призводять до економічної та інформаційної шкоди, але вони відрізняються за своїми правовими наслідками та потенціалом відновлення, що потребує спеціальних аналітичних і превентивних механізмів.

Напрями ідентифікації та кількісного оцінювання ризиків у цифровому середовищі є багатоаспектними та поєднують технічні, економічні й поведінкові виміри [9, с. 98–99]. На етапі ідентифікації аналітики знаходять потенційні джерела загроз: технічні вразливості в коді чи протоколах, людські помилки, фішингові схеми, інсайдерські зловживання або невідповідність нормативним вимогам. Кількісне оцінювання передбачає визначення ймовірності та очікуваного розміру втрат, часто з використанням імовірнісних моделей, симуляцій сценаріїв або статистичних висновків. Наприклад, у криптовалютних екосистемах кількісне оцінювання ризиків може охоплювати індекси волатильності й показники стійкості мережі, тоді як у контексті цифрових даних або онлайн-акаунтів воно може ґрунтуватися на моделях імовірності порушень та очікуваних витратах від вимушеного простою. Методологічна складність виникає через нематеріальність і динамічну природу цифрових активів, які залежать від технологічних середовищ, що швидко змінюються, і перебувають під впливом поведінкових факторів, таких як обережність користувачів, довіра до платформ і сприйнята цінність активу.

Методологічні засади аналізу ризиків у цифровій сфері вимагають комплексного підходу, який синтезує знання з кібербезпеки, правового регулювання та поведінкової економіки. З погляду кібербезпеки, аналіз ризиків полягає у виявленні технічних вразливостей та розробці стійких архітектур, які мінімізують поверхні атаки за допомогою шифрування, надмірності й протоколів автентифікації. Правове регулювання забезпечує основу для визначення цифрової власності, підзвітності та механізмів реституції у випадках несанкціонованого доступу або втрати, хоча глобальний характер цифрових активів часто створює юрисдикційну невизначеність. Поведінкова економіка, своєю чергою, підкреслює, як поведінкові упередження та особливості ухвалення рішень, такі як надмірна впевненість, небажання втрачати або стадна поведінка, формують індивідуальну й інституційну реакцію на цифрові ризики, впливаючи як на стратегії захисту від них, так і на стратегії пом'якшення їхніх наслідків. Тому ефективна методологія має охоплювати не лише об'єктивні показники ризику, а й суб'єктивні поведінкові моделі, які впливають на ймовірність ризикованих дій або запізнілої реакції на загрози.

У цьому контексті теоретико-методологічні засади аналізу ризиків втрати цифрових активів базуються на системній парадигмі, де взаємодіють технологічні, правові та людські фактори. Децентралізований і безмежний характер цифрової екосистеми вимагає адаптивних моделей, здатних врахувати взаємозалежності між технічною інфраструктурою та поведінкою користувачів. Кінцевою метою такого аналізу ризиків є не просто оцінка потенційних втрат, а створення проактивної системи запобігання, реагування й відновлення, яка забезпечить стійкість систем управління

цифровими активами та гарантуватиме безперервність цифрової цінності в постійно мінливому і взаємопов'язаному середовищі.

Життєвий цикл цифрового активу передбачає безперервний процес створення, управління, використання, передавання і, зрештою, застарівання або знищення цифрової форми цінності. Поняття життєвого циклу цифрового активу відображає динамічний і тимчасовий характер власності, контролю та економічної значущості ресурсів на основі даних у цифрових екосистемах [10, с. 127–128]. На відміну від традиційних матеріальних активів, цифрові активи існують виключно в межах технологічних інфраструктур, таких як розподілені реєстри, бази даних і хмарні системи, де їхня ідентичність, автентичність і функціональність залежать від криптографічної перевірки та протоколів доступу. Знаючи цей життєвий цикл, можна застосовувати структурований напрям до управління цифровими активами та оцінювати вразливості, які виникають на кожному з його етапів, де сходяться технологічні, юридичні й поведінкові ризики.

Формування або придбання цифрового активу знаменує початкову фазу його життєвого циклу, що охоплює процеси створення, токенізації або купівлі. Криптовалюта видобувається чи карбується шляхом обчислювальної валідації, токен, що не підлягає обміну, генерується за допомогою смарт-контрактів на блокчейні, а цифрові дані можуть генеруватися за допомогою алгоритмічних операцій або активності користувача. Ця фаза за своєю природою схильна до ризиків розробки й автентичності, зокрема помилкового кодування, шахрайської емісії або неперевіреного походження. Якість шифрування, прозорість протоколів створення та надійність механізмів початкової перевірки визначають довгострокову стабільність і цінність активу. Помилки або маніпуляції на цьому етапі можуть поширитися на все подальше існування активу, що призведе до втрати довіри або незворотної втрати легітимності.

Після формування актив переходить до етапу зберігання й адміністрування, де акцент зміщується в бік захисту, доступності та управління. Зберігання передбачає утримання активу в безпечному середовищі: цифрових гаманцях, децентралізованих мережах зберігання або на серверах — за підтримки механізмів шифрування, управління ключами та автентифікації особистості. Основними ризиками на цьому етапі є несанкціонований доступ, витік даних, апаратні збої та неналежне управління криптографічними обліковими даними. Суть парадоксу цифрового зберігання полягає в балансі між доступністю та захистом: надмірна централізація підвищує вразливість до масштабних атак, тоді як надмірна децентралізація може призвести до неможливості відновлення доступу в разі втрати ключа. Відповідно, адміністративні заходи, такі як автентифікація за допомогою декількох підписів, протоколи резервного копіювання й аудиторські записи, стають невіддільними елементами ефективного зниження ризиків.

Етап використання та обігу визначає функціональний строк служби цифрового активу, протягом якого він виконує своє економічне або інформаційне призначення. Активами можна вільно торгувати, ліцензувати їх, робити ставки або інтегрувати їх у цифрові екосистеми для створення цінності чи обміну даними. На цьому етапі виникають операційні та ринкові ризики. Транзакційні помилки, вразливості смарт-контрактів і системна нестабільність цифрових платформ можуть призвести до часткової або повної втрати активів. До того ж висока волатильність цифрових ринків посилює ризики щодо оцінки, а поведінкові фактори, такі як імпульсивна торгівля або дезінформація, можуть спотворити раціональне управління активами. Взаємодія між різними цифровими інфраструктурами також породжує проблеми сумісності та відповідності, що робить стандартизацію критично важливим фактором для безпечного й ефективного обігу [11].

Етап передання або успадкування розширює концепцію безперервності права власності в цифровому домені. Передання цифрового активу передбачає

автентифікацію та перевірку легітимності транзакції, що часто здійснюється за допомогою криптографічних підписів або децентралізованого узгодження. Успадкування, своєю чергою, стосується передання контролю між поколіннями або інституціями, коли первісний власник припиняє своє існування або втрачає операційну спроможність. Правові засади цифрового правонаступництва залишаються недостатньо розвиненими, що створює регуляторні та етичні проблеми. Пов'язані з цим ризики охоплюють несанкціоноване передання, суперечки щодо посмертного доступу й невідповідності між незмінністю блокчейну та спадковим правом. Тому для формалізації та убезпечення цього процесу дедалі частіше розглядаються такі механізми, як системи спадкування на основі смарт-контрактів або цифрові заповіти.

Завершальна фаза життєвого циклу, ліквідація, являє собою занепад або припинення актуальності чи існування цифрового активу. Видалення може відбуватися через навмисне видалення, закінчення строку дії цифрових прав, застарілість технології, що підтримує актив, або пошкодження даних. На цьому етапі виникають питання безпеки та сталості. Неправильне видалення може призвести до зловживань або несанкціонованого відновлення залишкових даних, тоді як незворотне знищення має забезпечити дотримання конфіденційності та регуляторних вимог. У розподілених системах видалення даних може бути технічно неможливим, що призводить до етичних дебатів про «право на забуття» в середовищах, які базуються на блокчейні [12].

Аналітично кожна стадія життєвого циклу цифрового активу являє собою специфічні конфігурації ризиків, які вимагають цілісного та адаптивного підходу. Ризики формування є переважно структурними, ризики зберігання — технічними та операційними, ризики використання — поведінковими і транзакційними, ризики передання – юридичними та процедурними, а ризики утилізації - етичними й регуляторними. Методологічний виклик полягає в тому, щоб інтегрувати ці аспекти в безперервну систему моніторингу ризиків, де завчасне виявлення і проактивне управління запобігають системним втратам або компрометації. Завдяки узгодженню управління цифровими активами з принципами кібербезпеки, цифрової етики та сталого управління даними з’являється можливість забезпечити збереження цілісності, функціональності й цінності цифрових активів протягом усього їхнього життєвого циклу, від створення до остаточної ліквідації.

Класифікація та аналітичне оцінювання ризиків втрати цифрових активів є важливим напрямом дослідження цифрової економіки, кібербезпеки та інформаційного менеджменту. В умовах, коли цифрові активи набувають щораз більшого фінансового та соціального значення, їх захист вимагає структурованого осмислення багатовимірних ризиків, які загрожують їхній цілісності, доступності та цінності. Ці ризики виникають на перетині технологічних вразливостей, людської поведінки, інституційних прогалин і ринкової нестабільності, утворюючи складну систему, яка потребує як якісного, так і кількісного аналізу. Ефективна класифікація ризиків дає змогу визначити походження, ймовірність і потенційний вплив несприятливих подій, а аналітичне оцінювання створює основу для розроблення адаптивних стратегій з метою запобігання або пом'якшення втрат.

Технічні ризики є однією з найбільш критичних категорій, що охоплює загрози, які виникають безпосередньо з технологічної інфраструктури, від якої залежать цифрові активи. Апаратні збої, такі як фізичний вихід із ладу пристроїв зберігання даних або несправності серверів, можуть призвести до незворотної втрати даних або тимчасової недоступності. Хакерські атаки використовують вразливості системи за допомогою шкідливих програм, програм-вимагачів або методів грубої сили, націлюючись на гаманці, біржі та бази даних. Фішингові кампанії обманом змушують користувачів розкривати конфіденційні облікові дані, а недоліки шифрування чи застарілі криптографічні алгоритми дають змогу несанкціоновано розшифровувати або

перехоплювати інформацію, пов'язану з активами. Динамічна й децентралізована природа систем на основі блокчейну ускладнює захист у режимі реального часу, вимагаючи постійних оновлень, тестування на проникнення та багаторівневих механізмів автентифікації [13].

Людський фактор залишається поширеним джерелом ризиків для цифрових активів, що випливає як із когнітивних, так і з поведінкових обмежень. Користувачі часто припускаються ненавмисних помилок під час транзакцій, наприклад надсилають активи на неправильні адреси або втрачають приватні ключі. Соціальна інженерія допомагає впливати на психологічні слабкості користувачів і видавати себе за іншу особу або емоційно переконувати їх, що призводить до розкриття конфіденційних даних чи авторизації шахрайських переказів. До того ж низький рівень цифрової грамотності збільшує вразливість до шахрайства та технологічних зловживань. Цей компонент аналізу ризиків наголошує на важливості освіти, інформаційних кампаній та орієнтованого на користувача дизайну систем безпеки, де інтуїтивно зрозумілі інтерфейси й автоматизовані сповіщення мінімізують наслідки людських помилок.

Організаційно-правові ризики відображають розбіжності між швидким технологічним розвитком цифрових активів і повільнішими темпами інституційної адаптації. У багатьох юрисдикціях відсутня узгоджена нормативно-правова база, що визначає права власності на цифрові активи, оподаткування та механізми правового захисту. Особливо актуальними є проблеми успадкування, оскільки цифрові активи часто залишаються недоступними для спадкоємців без попередніх домовленостей про розподіл ключів або систем успадкування на основі смарт-контрактів. Транскордонні обмеження та неузгодженість національних нормативно-правових актів ще більше ускладнюють повернення активів, дотримання законодавства і правозастосування. Правова невизначеність навколо токенів і криптовалют знижує довіру інвесторів і збільшує транзакційні витрати, створюючи середовище, в якому запобіжне правове структурування стає таким самим важливим, як і технічний захист.

Економічні ризики виникають через притаманну ринку цифрових активів волатильність і спекулятивний характер. Криптовалюти й токени схильні до швидких коливань вартості через ринкові настрої, макроекономічні зрушення та заяви регуляторних органів. Раптове падіння ліквідності може зробити активи непридатними для продажу, особливо це стосується нещодавно випущених токенів або токенів із низькою капіталізацією. Шахрайські інвестиційні схеми, такі як фінансова піраміда або операції «викачування і скидання», використовують інформаційну асиметрію децентралізованих ринків. Ці ризики вимагають застосування інструментів економічного моделювання, зокрема індексів волатильності, кореляційного аналізу та стрес-тестів ліквідності, для кількісного оцінювання потенційних фінансових ризиків та обґрунтування стратегій диверсифікації.

Інтегрована аналітична модель оцінювання ризиків забезпечує системну основу для визначення пріоритетів цих різноманітних категорій ризиків. Така модель поєднує аналіз імовірності, оцінку впливу та взаємозалежність ризиків у єдину матрицю, яка підтримує процес ухвалення рішень і планування заходів із мінімізації ризиків. У таблиці 1 наведено приклад узагальненої матриці оцінки ризиків для управління цифровими активами.

Управління та мінімізація ризиків, пов'язаних із втратою цифрових активів, є багатоаспектним процесом, який об'єднує технологічні, правові, організаційні та аналітичні інструменти в цілісну захисну екосистему [14]. У міру того як цифрові активи розширюються від криптовалют і токенів до інтелектуальної власності та ресурсів на основі даних, їхня безпека стає питанням стратегічного значення не лише для окремих користувачів, а й для корпорацій, фінансових установ та урядів. Складність цифрових інфраструктур у поєднанні зі швидкістю технологічних інновацій та глобальним

характером цифрових ринків вимагає застосування адаптивних, проактивних і міждисциплінарних механізмів, які забезпечують безперервність, конфіденційність і законний контроль над цифровими активами протягом усього їхнього життєвого циклу.

Таблиця 1

Узагальнена матриця оцінки ризиків для управління цифровими активами

Категорія ризиків				
Конкретний прояв	**Ймовірність (низька-висока)**	**Вплив на вартість активів (низька-висока)**	**Узагальнений рівень ризику**	**Рекомендовані заходи щодо зниження**
Технічні				
Апаратний збій, кібератака, дефект шифрування	Середня-Висока	Високий	Високий	Резервне сховище, оновлення шифрування, системи виявлення вторгнень
Людські				
Втрата ключів, фішинг, неналежне управління	Висока	Середній-Високий	Високий	Навчання користувачів, двофакторна автентифікація, моніторинг поведінки
Організаційні/правові				
Спори про право власності, питання спадкування, транскордонні бар'єри	Середня	Високий	Середньо-високий	Гармонізація правової бази, успадкування смарт-контрактів, комплаєнс-протоколи
Економічні				
Волатильність ринку, падіння ліквідності, шахрайство	Висока	Високий	Дуже високий	Диверсифікація портфеля, належна перевірка, регуляторний нагляд

Джерело: систематизовано за [11–13]

Технологічні механізми захисту формують основну лінію безпеки для запобігання несанкціонованому доступу та випадковій втраті. Багаторівневі системи автентифікації, що поєднують паролі, біометричні ідентифікатори та апаратну верифікацію, значно знижують імовірність викрадення персональних даних і шахрайських транзакцій. Технології резервного копіювання відіграють важливу роль у підтримці доступності активів шляхом реплікації даних між географічно розподіленими вузлами або захищеними хмарними середовищами, забезпечуючи стійкість до збоїв у роботі пристроїв або атак зловмисників із вимогами викупу. Апаратні гаманці, які ізолюють криптографічні ключі від онлайн-середовища, залишаються одними з найнадійніших засобів захисту криптовалют і токенів. Не менш важливим є шифрування, яке захищає цілісність і конфіденційність даних за допомогою передових криптографічних алгоритмів, що роблять цифрову інформацію недоступною для сторонніх осіб. Розвиток

постквантової криптографії є особливо актуальним у цьому контексті, оскільки нові обчислювальні можливості можуть поставити під загрозу поточні стандарти шифрування.

Правові інструменти сприяють інституціоналізації та легітимізації захисту цифрових активів. Цифрові заповіти є інноваційним правовим механізмом, який визначає передання прав власності та доступу до цифрових активів після смерті власника, вирішуючи таким чином проблему цифрового спадкування. Контракти про управління цифровими активами формалізують відносини між зберігачами та власниками, визначаючи зобов'язання, пов'язані зі збереженням, автентифікацією та відповідальністю в разі втрати. Регулювання ринку криптоактивів, прикладом якого є Регламент Європейського Союзу про ринки криптоактивів (MiCA), підвищує прозорість, захист інвесторів і стабільність ринку, встановлюючи вимоги до ліцензування, стандарти відповідності та зобов'язання щодо розкриття інформації для постачальників послуг. Ці правові інструменти не лише зменшують ризики щодо власності та правонаступництва, а й зміцнюють довіру до цифрової економіки, узгоджуючи приватні практики управління з державним наглядом [15].

Організаційні заходи є соціальною та процедурною основою управління ризиками. Формування політики з питань кібергігієни в установах і серед окремих користувачів забезпечує систематичне застосування безпечних моделей поведінки, таких як регулярне оновлення паролів, оновлення програмного забезпечення та ретельне оцінювання цифрової взаємодії. Підвищення обізнаності користувачів за допомогою освітніх програм, семінарів та ігрових симуляцій допомагає протидіяти соціальній інженерії, фішингу і психологічним маніпуляціям, які часто призводять до інцидентів зі збитками.

Аналітичні системи моніторингу ризиків є найбільш динамічним і прогнозованим елементом сучасного управління цифровими активами. Штучний інтелект і технології великих даних дають змогу безперервно аналізувати величезні потоки транзакційних і поведінкових даних для виявлення аномалій, ранніх ознак вторгнення і прогнозування нових загроз. Алгоритми машинного навчання підвищують точність прогнозування, адаптуючись до нових моделей атак і мінливих ринкових умов. Аналіз великих даних іще більше полегшує кореляцію технічних, фінансових і соціальних показників, пропонуючи розуміння потенційних вразливостей у цифрових екосистемах у режимі реального часу.

Міжнародний досвід надає важливі орієнтири для побудови ефективних систем захисту цифрових активів. Такі країни, як Швейцарія, Сінгапур і Японія, створили передові моделі регулювання й зберігання цифрових активів, які поєднують правову ясність, технологічні інновації та галузеве саморегулювання. У США інтеграція в цифрові фінанси стандартів кібербезпеки Національного інституту стандартів і технологій (NIST) підвищує інституційну стійкість, а естонська модель електронного урядування демонструє потенціал державних систем цифрової ідентифікації для безпечної автентифікації та адміністрування активів. Порівняльний аналіз цих практик підкреслює важливість гармонізації технологічного розвитку з правовими та організаційними рамками для забезпечення глобальної сумісності й довіри [16, с. 337–338].

У таблиці 2 узагальнено основні категорії інструментів для управління ризиками втрати цифрових активів та їх мінімізації, проілюстровано їхні функції, практичне застосування та превентивні ефекти. Як бачимо, ефективне управління ризиками, пов’язаними з цифровими активами, не може ґрунтуватися на ізольованих технологічних чи правових заходах. Натомість воно вимагає постійної координації між технічними експертами, політиками та користувачами, підкріпленої адаптивними аналітичними системами, здатними вчитися на вітчизняному й міжнародному досвіді. Завдяки синтезу цих інструментів екосистеми цифрових активів будуть розвиватися в

напрямку більшої стійкості, прозорості та сталості, гарантуючи, що цифрові цінності залишаються захищеними в глобальному інформаційному просторі, який швидко трансформується.

Таблиця 2

Основні категорії інструментів для управління та мінімізації ризиків втрати цифрових активів

Категорія інструментів	**Приклади та механізми**	**Основна функція**	**Очікуваний вплив на зниження ризиків**
Технологічні	Багаторівнева автентифікація, апаратні гаманці, резервне копіювання, шифрування	Технічний захист та цілісність даних	Мінімізація несанкціонованого доступу та втрати даних
Юридичні	Цифрові заповіти, контракти з управління активами, регулювання ринку криптоактивів	Юридична перевірка та безперервність володіння	Зменшення спадкових та юрисдикційних ризиків
Організаційні	Політика кібергігієни, навчання користувачів, внутрішні аудити	Запобігання поведінковим та процедурним ризикам	Зменшення кількості людських помилок та інцидентів соціальної інженерії
Аналітичні	Моніторинг на основі ШІ, аналіз великих даних, системи виявлення аномалій	Прогностична ідентифікація загроз	Раннє попередження та запобігання масштабним втратам

Джерело: систематизовано за [13–20]

Перспективи розвитку аналітики ризиків у сфері цифрових активів тісно переплітаються з прискоренням темпів технологічних інновацій, розширенням глобальних цифрових ринків і зростанням залежності суспільства від електронних форм вартості. Нові тенденції в технологіях управління цифровими ризиками свідчать про перехід до предиктивних, адаптивних та інтегративних систем, здатних передбачати загрози й реагувати на них у режимі реального часу. Для виявлення аномалій, запобігання несанкціонованому доступу та оптимізації управління активами активно досліджуються і впроваджуються передові алгоритми машинного навчання, протоколи моніторингу на основі блокчейну та децентралізовані рішення для ідентифікації особи. Інтеграція цих технологій дає змогу автоматизувати процеси оцінювання ризиків і розширює можливості моделювання складних сценаріїв, включаючи каскадні ефекти кібератак, ринкових потрясінь або системних збоїв. До того ж конвергенція штучного інтелекту з інтернетом речей (IoT) та периферійними обчисленнями полегшує моніторинг цифрових активів, які щораз більше вбудовуються у взаємопов'язані фізичні й віртуальні екосистеми.

Стратегічний вимір майбутнього розвитку полягає в підвищенні цифрової грамотності як важливої основи для безпечного володіння та управління активами. Оскільки користувачі й організації функціонують у дедалі складнішому цифровому середовищі, їхня здатність розпізнавати загрози, впроваджувати методи безпеки та ухвалювати обґрунтовані рішення щодо використання і передання цифрових активів стає вирішальним фактором у зменшенні ризиків. Освітні програми, інформаційні кампанії та ініціативи з професійного навчання, спрямовані на розуміння принципів

криптографії, безпечних транзакцій та кібергігієни, стають обов'язковими компонентами комплексного управління ризиками. Цифрова грамотність не лише зменшує ймовірність людських помилок і вразливість до соціальної інженерії, а й сприяє впровадженню технічних та організаційних заходів захисту, створюючи культуру усвідомленого й відповідального володіння цифровими активами [21].

Висновки

У результаті проведеного дослідження встановлено, що ризики втрати цифрових активів мають багатовимірний характер і проявляються на всіх етапах їхнього життєвого циклу, від формування до утилізації. Визначено, що на ранніх етапах життєвого циклу домінують технологічні ризики, пов'язані з недосконалістю протоколів шифрування, помилками в проєктуванні цифрових систем і кіберзагрозами. У процесі зберігання та використання активів вагомими є людський фактор і організаційні недоліки: неналежне управління ключами доступу, низький рівень цифрової грамотності користувачів, недотримання політик кібергігієни. На етапах передання, спадкування або ліквідації активів основними викликами стають правова неврегульованість, юрисдикційні розбіжності та відсутність єдиних механізмів верифікації права власності.

Отримані результати підтверджують, що ефективне управління ризиками втрати цифрових активів потребує комплексного підходу, в якому технологічний захист має доповнюватися нормативно-правовим забезпеченням і підвищенням цифрової компетентності користувачів. Впровадження багаторівневих систем автентифікації, смарт-контрактів для спадкування цифрових активів, а також використання штучного інтелекту для моніторингу та прогнозування кіберзагроз формує основу для створення стійкої інфраструктури цифрової безпеки. Таким чином, дослідження доводить необхідність системного підходу до аналітики ризиків, пов'язаних із цифровими активами, орієнтованого на постійний моніторинг, адаптацію та взаємодію між державою, бізнесом і користувачами. Перспективи подальших наукових досліджень полягають у розробленні інтелектуальних моделей прогнозування ризиків із використанням великих даних і машинного навчання для підвищення ефективності управління цифровими активами.

Список використаних джерел

1. Коростін О. Оптимізація маршрутів морських перевезень за допомогою штучного інтелекту: аналіз можливостей та викликів. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво.* 2024. № 56. С. 31–38. DOI: https://doi.org/10.36910/6775-2524-0560-2024-56-03.

2. Гонак І. М. Ризики функціонування криптовалютного бізнесу. *Вісник Херсонського державного університету. Серія: Економічні науки.* 2021. № 44. С. 81-86. DOI: https://doi.org/10.32999/ksu2307-8030/2021-44-12.

3. Волосович С. В., Нападовський І. І. Ризики криптовалютних активів та можливості їх страхування. *Modern Economics*. 2024. №43. С. 24–30. DOI: https://doi.org/10.31521/modecon.V43(2024)-03.

4. Москвін Б. Ю. Перспективи розвитку правового регулювання цифрових активів в Україні. *Київський часопис права.* 2024. № 2. С. 184–189. DOI: https://doi.org/10.32782/klj/2024.2.27.

5. Levchenko M. Marketing and advertising strategies for business expansion in emerging markets: integrating outdoor media for maximum reach. *Актуальні питання економічних наук.* 2025. № 12. DOI: https://doi.org/10.5281/zenodo.15779284.

6. Зінченко М., Мостовенко О., Корсун І. Цифрові гроші: переваги та ризики для економіки. *Просторовий розвиток*. 2024. № 9. С. 327–335. DOI: https://doi.org/10.32347/2786-7269.2024.9.327-335.

7. Мехович Є. М. Інтеграція цифрових фінансових активів у розрахунково-платіжну систему та запобігання можливих ризиків (прогнозні підходи). *Енергозбереження. Енергетика. Енергоаудит.* 2024. № 11 (202). С. 64–82. DOI: https://doi.org/10.20998/2313-8890.2024.11.05.

8. Ситнік Є. Теоретичні основи впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства. *Вчені записки Університету «КРОК».* 2025. № 1 (77). С. 371–378. DOI: https://doi.org/10.31732/2663-2209-2025-77-371-378.

9. Канигін С. М. Великі дані в управлінні фінансами підприємства. *Економіка, управління та адміністрування.* 2024. № 3 (109). С. 97–104. DOI: https://doi.org/10.26642/ema-2024-3(109)-97-104.

10. Защипас С. М. Фундаментальні поняття віртуальних активів та механізм їх функціонування. *Економіка, управління та адміністрування*. 2025. № 2 (112). С. 121–134. DOI: https://doi.org/10.26642/ema-2025-2(112)-121-134.

11. Гурін Б. Теоретико-правова характеристика криптовалют як концептуальних засобів обороту та оцінка їх ролі для розвитку криптоіндустрії в Україні. *Академічні візії.* 2023. № 25. DOI: https://doi.org/10.5281/zenodo.10148228.

12. Боркович В. В. Фінансові, інституційні та нормативно-правові основи функціонування криптовалют у сучасній економіці. *Актуальні питання економічних наук.* 2025. № 11. DOI: https://doi.org/10.5281/zenodo.15490630.

13. Ставерська Т. О., Глущенко І. А., Лисак Г. Г. Аналіз переваг і ризиків розроблення блокчейн-платформ для фінансування стартапів. *Актуальні питання економічних наук.* 2025. № 8. DOI: https://doi.org/10.5281/zenodo.14792528.

14. Підхомний О., Приймак І., Пономаренко О. Формування парадигми управління ризиками у сфері криптострахування. *Економіка та суспільство*. 2021. № 34. DOI: https://doi.org/10.32782/2524-0072/2021-34-50.

15. Перебийніс Д. Правові аспекти та майбутнє регулювання електронних фінансових інструментів у процесі залучення капіталу. *Економіка та суспільство.* 2025. № 71. DOI: https://doi.org/10.32782/2524-0072/2025-71-149.

16. Дарчик Г. М. Сучасний стан правового регулювання криптовалюти в Україні. Зарубіжний досвід регулювання ринку криптовалют. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2025. № 2 (87). С. 335–340. DOI: https://doi.org/10.24144/2307-3322.2025.87.2.50.

17. Люшенко Д. І., Шарафан Р. В., Туголуков О. Є. Моделювання процесів спадкування цифрових активів із використанням технологій blockchain. *Академічні візії.* 2025. № 47. DOI: https://doi.org/10.5281/ZENODO.17189081.

18. Шарафан Р. В., Туголуков О. Є. Інформаційні системи для управління цифровою спадщиною та їхня інтеграція у правові процеси. *Український політико-правовий дискурс.* 2025. № 15. DOI: https://doi.org/10.5281/zenodo.17197093.

19. Люшенко Д., Шарафан Р., Туголуков О. Інформаційні технології у створенні «цифрових сейфів» для зберігання спадкових активів. *Наука і техніка сьогодні*. 2025. № 9 (50). С. 1304 – 1321. DOI: https://doi.org/10.52058/2786-6025-2025-9(50)-1304-1321.

20. Sherifi I., Lebid O., Goncharova O., Drobyazko S., Sidko I. Financial risks of business management of cryptocurrency operations. *TEM Journal.* 2024. Vol. 13, № 1. P. 355–364. DOI: https://doi.org/10.18421/TEM131-37.

21. Laurențiu-George D. I. N. U. Using cryptocurrencies, a management strategy for the future. *Internal Auditing & Risk Management.* 2022. Vol. 65, № 1. P. 19–32. URL: https://ideas.repec.org/a/ath/journl/v65y2022i1p19-32.html.