УДК 004.056.5:336.71

Трет'як Ігор Олександрович
здобувач ступеня доктора філософії зі спеціальності
072 Фінанси, банківська справа та страхування
Сумського державного університету
Tretiak Ihor
PhD Candidate in Specialty
072 Finance, Banking and Insurance
Sumy State University
ORCID: 0009-0003-2264-8430

DOI: 10.25313/2520-2294-2025-11-11603

КІБЕРРИЗИКИ ДЕЦЕНТРАЛІЗОВАНИХ ФІНАНСІВ ЯК ФАКТОР СИСТЕМНОЇ ВРАЗЛИВОСТІ ЦИФРОВОЇ ЕКОНОМІКИ

CYBER RISKS OF DECENTRALIZED FINANCE AS A FACTOR OF SYSTEMIC VULNERABILITY IN THE DIGITAL ECONOMY

Анотація. *Вступ. Децентралізовані фінанси (DeFi) формують нову парадигму цифрової економіки, у якій управління активами, довіра та виконання угод реалізуються за допомогою смартконтрактів і блокчейн-технологій. Відмова від традиційних посередників і перехід до алгоритмічної автономії створили передумови для побудови відкритої, прозорої та інклюзивної фінансової системи. Водночас така децентралізація посилює вразливість до кіберзагроз, що проявляються у формах атак на протоколи, маніпуляцій даними, експлуатації вразливостей блокчейн-мостів та ораклів. Втрата стабільності хоча б одного з компонентів екосистеми може спричинити каскадні ефекти у пов'язаних протоколах, що перетворює технічні інциденти на системні ризики. У цих умовах виникає потреба в новій моделі управління безпекою – кіберстійкості, яка забезпечує здатність DeFi-протоколів ідентифікувати, передбачати, локалізовувати та долати загрози, зберігаючи цілісність і функціональність фінансової інфраструктури..*

Мета. Метою дослідження є наукове обґрунтування концепції кіберрстійкості децентралізованих фінансів і розроблення цілісної моделі, що поєднує технологічні, регуляторні та поведінкові інструменти підвищення їхньої спроможності протидіяти кіберризикам і забезпечувати стабільність фінансової екосистеми.

Матеріали і методи. Методологічною основою дослідження є системний та міждисциплінарний підходи, які поєднують інструменти фінансової теорії, кібербезпеки та цифрової економіки. Для досягнення мети використано методи структурно-функціонального аналізу – з метою виявлення взаємозв'язків між технологічними, регуляторними й поведінковими елементами DeFi-екосистеми. Метод порівняльного аналізу застосовано для оцінки міжнародних підходів до управління кіберризиками у сфері децентралізованих фінансів, зокрема з урахуванням стандартів MiCA, FATF, DAC8 та CARF. Метод логіко-аналітичного узагальнення використано для формування концептуальної моделі кіберстійкості DeFi та визначення її етапів – ідентифікації, прогнозування, реакції й відновлення. Елементи графічного моделювання застосовано для візуалізації взаємозв'язків між рівнями та фазами кіберстійкості. Інформаційну базу дослідження становлять наукові публікації, аналітичні звіти міжнародних організацій, нормативно-правові документи ЄС та емпіричні дані щодо динаміки кіберінцидентів у DeFi-секторі за 2020–2025.

Результати. У статті обґрунтовано, що децентралізовані фінанси є не лише інноваційною формою організації фінансової діяльності, а й середовищем з підвищеною концентрацією кіберризиків, які можуть трансформуватися у системні загрози для цифрової економіки. Доведено, що традиційні підходи до безпеки, орієнтовані на захист від інцидентів, є недостатніми в умовах автономного функціонування смартконтрактів і відсутності централізованого контролю. На основі аналізу механізмів атак показано, що найбільших втрат зазнають протоколи з високою ліквідністю та міжланцюговими зв'язками. Запропоновано концептуальну модель кіберстійкості DeFi, яка охоплює чотири послідовні етапи – ідентифікацію, прогнозування, реакцію та відновлення – і функціонує у межах трьох взаємопов'язаних рівнів: технологічного, регуляторного та поведінкового. Модель забезпечує перехід від реактивної до проактивної безпеки, де системи здатні

самостійно виявляти аномалії, обмежувати вплив атак і відновлюватися після інцидентів без зовнішнього втручання. Доведено, що впровадження цієї парадигми створює умови для формування саморегульованих фінансових екосистем, у яких безпека є невід'ємним атрибутом технологічного дизайну протоколів.

Перспективи. Запропоновано стратегічні напрями підвищення кіберстійкості децентралізованих фінансів, що передбачають поєднання технологічних інновацій із регуляторною координацією. Серед ключових напрямів – розроблення алгоритмічних механізмів самозахисту протоколів, інтеграція систем штучного інтелекту для раннього виявлення загроз, а також впровадження стандартів кібернагляду на основі міжнародних ініціатив MiCA, FATF, DAC8 і CARF. Перспективним є формування єдиного індексу кіберризику DeFi (DCRI), який дозволить здійснювати кількісну оцінку рівня безпеки децентралізованих протоколів і забезпечить порівнянність даних на глобальному рівні. Важливою умовою розвитку кіберстійкості є створення децентралізованих страхових пулів (DAO Insurance Pools) та розбудова партнерств між розробниками, аудиторами коду й регуляторами. Реалізація цих заходів сприятиме становленню саморегульованої фінансової архітектури, де кібербезпека стає не зовнішньою вимогою, а внутрішнім механізмом сталого функціонування DeFi-екосистеми.

Ключові слова: *DeFi, кіберризики, кіберстійкість, смартконтракти, блокчейн, FinTech 4.0, цифрова безпека, регулювання криптоактивів, DAO, MiCA, FATF, саморегульовані системи.*

Summary. *Introduction. Decentralized finance (DeFi) constitutes a transformative paradigm of the digital economy, where asset management, trust, and transaction execution are governed by smart contracts and blockchain infrastructure. The elimination of traditional intermediaries and the transition to algorithmic autonomy have enabled the emergence of an open, transparent, and inclusive financial system. However, this decentralization simultaneously increases exposure to cyber threats, including protocol exploits, oracle manipulation, and cross-chain vulnerabilities. The instability of a single protocol can trigger cascading failures across interconnected networks, turning technical incidents into systemic financial risks. Hence, a new security governance framework – cyber-resilience – is required to ensure DeFi's ability to identify, anticipate, contain, and recover from cyber threats while maintaining the integrity and continuity of its financial infrastructure.*

Purpose. The study aims to conceptualize cyber-resilience in decentralized finance and develop an integrated model combining technological, regulatory, and behavioral mechanisms to strengthen DeFi's capacity to withstand cyber risks and sustain systemic stability.

Materials and Methods. The research methodology is grounded in systemic and interdisciplinary approaches integrating financial theory, cybersecurity, and digital economy tools. Structural-functional analysis was employed to examine the interrelations among technological, regulatory, and behavioral components of DeFi ecosystems. Comparative analysis was applied to assess international practices of cyber-risk management under the frameworks of MiCA, FATF, DAC8, and CARF. Logical-analytical synthesis was used to construct a conceptual model of DeFi cyber-resilience encompassing four phases – identification, prediction, response, and recovery – while graphical modeling techniques were utilized to visualize their interconnections. The empirical foundation includes scientific publications, policy reports, EU regulations, and statistical data on cyber incidents in DeFi from 2020 to 2025.

Results. The study demonstrates that DeFi is both an innovative financial architecture and a high-risk environment where cyber incidents may escalate into systemic disruptions. Conventional security frameworks focused on incident response are inadequate in decentralized settings characterized by autonomous smart-contract execution. An analysis of major attack vectors – flash-loan exploits, oracle manipulation, and bridge vulnerabilities – reveals that highly liquid and cross-chain protocols face the greatest exposure. The proposed model of DeFi cyber-resilience integrates four functional stages within three interrelated levels – technological, regulatory, and behavioral – providing a transition from reactive to proactive security. Within this framework, DeFi systems are envisioned as self-adaptive entities capable of detecting anomalies, mitigating threats autonomously, and recovering without centralized intervention.

Perspectives. The paper outlines strategic directions for enhancing DeFi cyber-resilience, emphasizing the fusion of technological innovation and regulatory harmonization. Priority measures include the development of algorithmic self-defense mechanisms, AI-based threat detection, and the implementation of supervisory standards aligned with MiCA, FATF, DAC8, and CARF. Establishing a unified DeFi Cyber-Risk Index (DCRI) is proposed to enable quantitative assessment and global benchmarking of protocol security. Further, the creation of decentralized insurance pools (DAO Insurance Pools) and collaborative frameworks among developers, auditors, and regulators are identified as key enablers of self-regulated financial ecosystems. The proposed paradigm positions cybersecurity as an intrinsic design feature of DeFi protocols, ensuring sustainability and trust within the evolving digital financial architecture.

Key words: *decentralized finance (DeFi), cyber risks, cyber-resilience, smart contracts, blockchain, FinTech 4.0, digital security, crypto-asset regulation, DAO, MiCA, FATF, self-regulated systems.*

Постановка проблеми. Розвиток децентралізованих фінансів став одним із ключових проявів трансформації глобального фінансового ринку в умовах цифрової економіки. Завдяки використанню блокчейн-технологій, смартконтрактів і алгоритмічного управління, DeFi забезпечує безпосередню взаємодію користувачів без участі традиційних фінансових посередників. Водночас відсутність централізованого контролю, прозорі вихідні коди та відкритість мережевої інфраструктури створю-

ють передумови для виникнення нової категорії ризиків — кіберризиків, які мають комплексний, багаторівневий і системний характер.

Особливу загрозу становлять атаки на смарт-контракти, маніпуляції ораклами і вразливості кросчейн-мостів, наслідком яких можуть бути не лише фінансові втрати, а й дестабілізація цілих протоколів або мереж. У цьому контексті традиційні підходи до кібербезпеки, що передбачають централізоване реагування на інциденти, виявляються неефективними для DeFi-систем, які функціонують автономно.

Отже, постає потреба в новій концепції захисту — кіберстійкості децентралізованих фінансів, що поєднує технологічні, регуляторні та поведінкові аспекти. Така концепція має забезпечити здатність DeFi-протоколів ідентифікувати, прогнозувати, локалізовувати та долати кіберзагрози, зберігаючи цілісність фінансової екосистеми та довіру користувачів.

Аналіз останніх досліджень і публікацій. Дослідження цифрової трансформації фінансових ринків і становлення DeFi сформували міждисциплінарне поле, що охоплює архітектуру протоколів, управління ризиками та кібербезпеку. Узагальнюючі праці підкреслюють багаторівневу природу ризиків і наявність прихованих точок централізації, які підвищують ймовірність маніпуляцій і технічних збоїв [3; 6; 22; 23]. Огляди центральних банків акцентують на «ілюзії децентралізації» та непрямих каналах передавання ризику через стейблкоїни, біржі та платіжні шлюзи, що створює потенційні загрози для регульованого сектору [4; 17].

Емпіричний пласт літератури фіксує ескалацію інцидентів безпеки: домінування атак типу flash-loan, маніпуляцій ораклами, експлойтів блокчейн-мостів і помилок у смартконтрактах [14; 26]. Методичні підходи варіюються від експертних схем оцінювання ризиків (fuzzy-AHP) до систематичних оглядів, що класифікують технічні, фінансові та правові загрози [5; 15; 16]. Міжгалузеві студії Web 3.0 описують алгоритми виявлення аномалій і детектори на основі ML/AI [19; 20], тоді як регуляторні роботи аналізують AML/CFT-ризики, взаємодію CeFi/DeFi та гармонізацію з MiCA і FATF [10; 22].

Попри прогрес, зберігаються ключові прогалини: фрагментарність підходів (розділення технічних, регуляторних і поведінкових аспектів без інтеграції в єдину рамку управління ризиком), відсутність уніфікованих метрик кількісного виміру кіберризику DeFi індексного типу, а також недопрацьовані механізми поєднання автоматизованої реакції смартконтрактів із прозорими компенсаційними інструментами DAO [11; 15; 26]. Саме ці розриви обґрунтовують запропоновану в роботі інтегровану концепцію кіберстійкості DeFi як замкненого циклу «ідентифікація — прогнозування — реакція — відновлення» у зв'язці з технологічним, регуляторним і поведінковим рівнями [3; 4; 11; 17; 26].

Метою статті є наукове обґрунтування концепції кіберстійкості DeFi, що поєднує технологічні, регуляторні й поведінкові механізми забезпечення безпеки децентралізованих фінансових протоколів.

Для досягнення цієї мети поставлено такі основні **завдання**:

– дослідити природу та типологію кіберризиків у DeFi-середовищі;
– узагальнити міжнародний досвід регуляторного реагування на кіберризики у сфері децентралізованих фінансів;
– запропонувати концептуальну модель кіберстійкості DeFi;
– визначити ключові структурні рівні кіберстійкості та їхні взаємозв'язки в межах децентралізованої екосистеми;

Виклад основного матеріалу. Децентралізовані фінанси (DeFi) є одним із найдинамічніших вимірів фінансової інновації, що поєднує технологічну автономність, відкритість коду та економічну самоорганізацію. На відміну від централізованих фінансів (CeFi), де контроль, гарантування й збереження активів забезпечують банки, біржі та інші посередники, DeFi ґрунтується на смартконтрактах — самовиконуваних програмах, які автоматично реалізують умови угоди без участі третьої сторони. Такий зсув трансформує природу фінансової довіри: від юридично-інституційних гарантій до алгоритмічних механізмів, переозначуючи межі відповідальності та ризику в цифровій економіці [14].

У цьому контексті DeFi постає не лише інструментом інновації, а й каталізатором цифрової трансформації — переходом від автоматизації операцій до алгоритмічної автономії. Децентралізовані протоколи формують нову фінансову архітектуру, у якій нагляд, аудит і управління кодуються в алгоритми, а взаємодія відбувається без посередників; відтак DeFi стає ядром цифрової економіки нового покоління з відкритими даними, смартрегулюванням і глобальною інтеграцією фінансових потоків. Перехід від електронізації транзакцій до саморегульованих екосистем базується на поєднанні цифрових активів, штучного інтелекту та блокчейна як фундаменті нової моделі економічної довіри [6].

Сутність DeFi полягає не лише у децентралізації транзакцій, а й у формуванні нового типу фінансової архітектури, у якій основою довіри стає код, а не інституція. За висновками К. Гоголя (Gogol, K.), К. Кіллера (Killer, C.) та М. Шлоссера (Schlosser, M.) [14], екосистема DeFi функціонує як багаторівнева система ризиків, де протокольний, транзакційний і ринковий рівні взаємодіють у межах спільного інформаційного простору. Ця взаємодія утворює складну мережеву архітектуру цифрової фінансової екосистеми, у якій інформаційні, технологічні та економічні процеси поєднуються в єдину логіку алгоритмічного управління. При цьому навіть формально децентралізовані платформи нерідко

містять приховані точки централізації — контроль адміністративних ключів (admin keys) або залежність від централізованих постачальників даних (data oracles), що може провокувати маніпуляції ринковими показниками та підвищувати вразливість системи [26]. Таким чином, DeFi демонструє не лише еволюцію фінансових інструментів, а й перехід до нової цифрової логіки фінансової організації, у якій довіра, контроль і ризик реалізуються безпосередньо у програмному коді.

Науковий інтерес до DeFi дедалі частіше зміщується від технічного рівня до системного аналізу ризиків. С. Ауф'єро (Aufiero, S.), С. Бартолуччі (Bartolucci, S.), Ф. Каччолі (Caccioli, F.) та П. Віво (Vivo, P.) [7] показують, що DeFi-ризики мають як мікроскопічний характер — помилки у коді, вразливості блокчейн-мостів (bridge exploits), так і макроскопічний -системні ефекти, здатні поширюватися на весь фінансовий сектор. Взаємозалежність децентралізованих протоколів означає, що навіть одна локальна атака може запустити ефект ланцюгової реакції у глобальному фінансовому середовищі, особливо коли протоколи зв'язані через стабількоїни або DeFi-біржі. Це дозволяє трактувати DeFi як інфраструктурний елемент цифрової економіки, де поєднуються автономія та системна взаємозалежність, і де виникають нові типи системних ризиків — мережеві, алгоритмічні та поведінкові.

Дослідження Ф. Бекемайєра (Bekemeier, F.) розкриває феномен оманливої впевненості (deceptive assurance), коли користувачі переоцінюють технологічну безпеку децентралізованих систем лише через усунення людського фактору. Насправді децентралізація не усуває ризики, а змінює їхню природу — від людських помилок до системних та кодувальних збоїв; це вимагає моделей оцінювання, що враховують алгоритмічну поведінку й мережеву взаємозалежність протоколів. Дотичне поняття системної вразливості описує здатність локальних збоїв перерости у макроефекти через канали ліквідності, біржі й стейблкоїни [9].

У взаємодії DeFi–TradFi проявляється парадокс децентралізації: що вищий рівень автономності, то складнішими стають контроль, аудит і верифікація ризиків. Додатково на це нашаровується явище псевдодецентралізації (*Fake-DeFi*), коли формально відкриті протоколи фактично зберігають контроль у розробників чи великих інвесторів, породжуючи регуляторну невизначеність і підрив довіри користувачів [11].

Розвиток DeFi супроводжується становленням децентралізованих форм управління, що реалізуються через DAO (Decentralized Autonomous Organization). Як зазначає В. Дорайсамі (Doraisamy, V.), колективна автономія за відсутності централізованих механізмів безпеки породжує соціотехнічні ризики: конфлікти інтересів, неефективне ухвалення рішень і затримки реагування на інциденти. Отже, у DeFi-технологічні вразливості тісно переплітаються з поведінковими чинниками, формуючи гібридний ризиковий простір [13].

Загальна структура ризиків у DeFi, за результатами синтезу підходів [3; 4; 6; 17; 22; 23], може бути представлена у вигляді чотирьох основних груп:

- технологічні ризики — пов'язані з вразливостями коду, смартконтрактів та ораклів;
- системні ризики — поширення локальних збоїв через взаємопов'язані протоколи;
- поведінкові ризики — колективні рішення, що підсилюють волатильність;
- регуляторні ризики — невизначеність статусу активів і протоколів у законодавстві.

Розуміння цих ризиків дозволяє трактувати DeFi як систему, де стійкість визначається не відсутністю збоїв, а здатністю швидко відновлюватися. Разом вони формують мережевий контур кіберуразливості, де одиничний збій може спричинити каскад у пов'язаних протоколах. Звідси — інтегрований кіберекономічний підхід: DeFi як самоорганізована система на перетині технологій, стимулів і поведінки, у якій ризик є ендогенним елементом алгоритмічної довіри, а код виконує не лише операційну, а й нормативну функцію. Необхідні методології поведінкової кібербезпеки, що враховують взаємодію людських рішень і машинних алгоритмів [26].

Концептуальна модель DeFi як рівноваги між автономністю, довірою та ризиком відображає механізм самоорганізації децентралізованих фінансів, де технологічні, соціальні та безпекові чинники взаємодіють у динамічному балансі. Автономність забезпечується алгоритмічним управлінням через смартконтракти та DAO, що усувають посередників і створюють умови для саморегуляції системи. Проте така самостійність можлива лише за умови алгоритмічної довіри — впевненості користувачів у надійності коду, децентралізованому механізмі консенсусу та прозорості транзакцій. Саме довіра перетворюється на ключовий ресурс, який підтримує функціонування автономних протоколів і визначає темп їхнього розвитку.

Водночас ризик є зворотним боком автономності — із зменшенням централізованого контролю зростають можливості для помилок, атак та маніпуляцій. Коли ризики перевищують рівень прийнятної довіри, система втрачає стійкість і переходить у фазу адаптації, змінюючи механізми безпеки та управління. Отже, модель відображає циклічну взаємодію трьох сил: довіра породжує автономність, автономність — ризик, а ризик обмежує або переформатовує довіру. У цьому полягає концептуальна сутність DeFi — це не просто набір технологій, а жива система рівноваги, де стабільність досягається через постійну взаємодію між алгоритмами, користувачами та ризиковим середовищем.

Аналітичний огляд кіберзагроз у DeFi має поєднувати кількісний аналіз атак, оцінку збитків

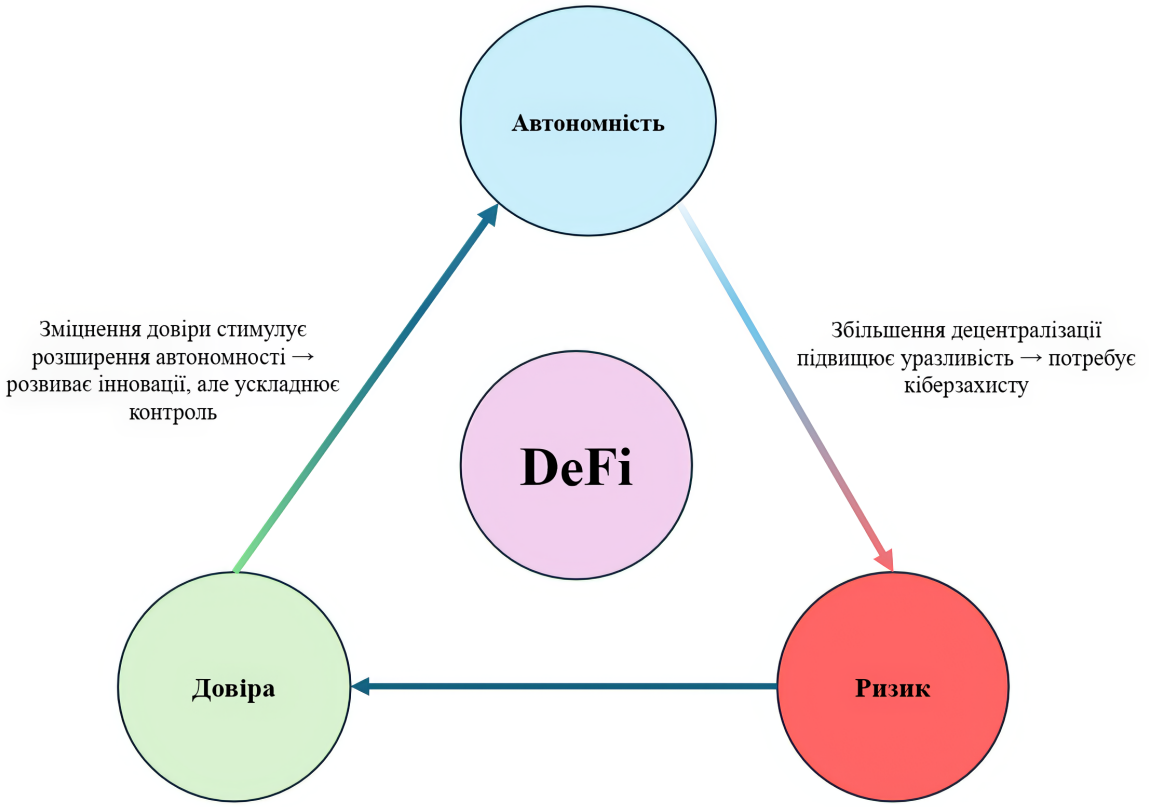

Рис. 1. Концептуальна модель DeFi як рівноваги між автономністю, довірою та ризиком
Джерело: побудовано автором на основі [3; 4; 6; 17; 22; 23]

і зіставлення з TradFi. За Дж. Маккеєм (McKay, J.) [20] та В. Семеренською (Semerenska, V.) [24], у 2017–2025 рр. втрати зросли з ~150 млн. дол. до понад 6 млрд. дол. США. Найуразливіші — lending-протоколи, AMM та блокчейн-мости; зростає середній збиток на інцидент і частота каскадних подій через спільні оракули та пули ліквідності. Фіксується кластеризація у часі, кореляція з ринковою волатильністю та падінням TVL ((Total Value Locked), а втрати концентруються у «системних» протоколах. На відміну від TradFi, швидкість ончейн і відсутність єдиного адміністратора посилюють поширення ефектів, що підсилює потребу в інтегрованих механізмах кіберстійкості.

Наведені кейси ілюструють найбільші інциденти у DeFi за останні роки та типові вектори зламу:

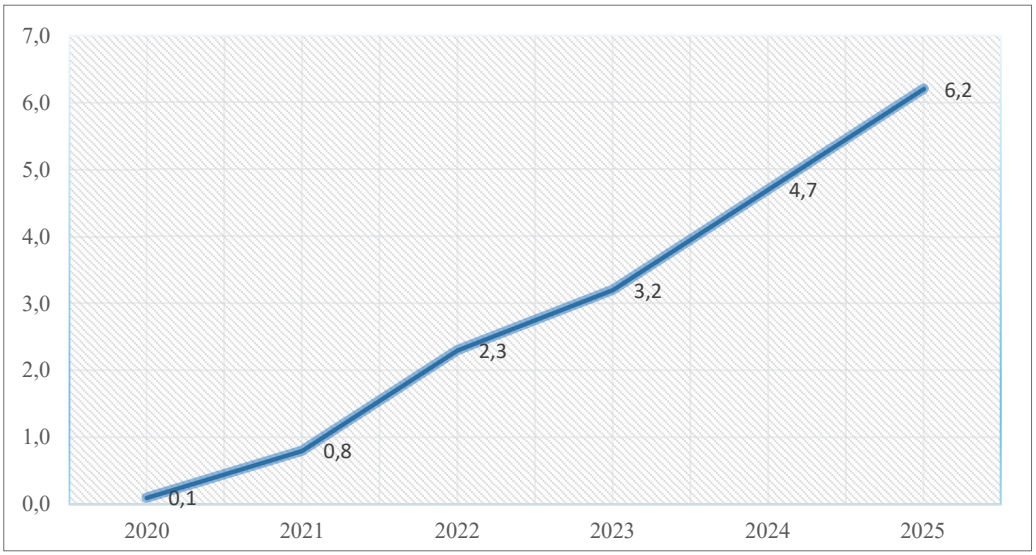

Рис. 2. Динаміка фінансових втрат у DeFi-секторі 2017–2025 рр.
Джерела: [13; 14; 20; 24; 26]

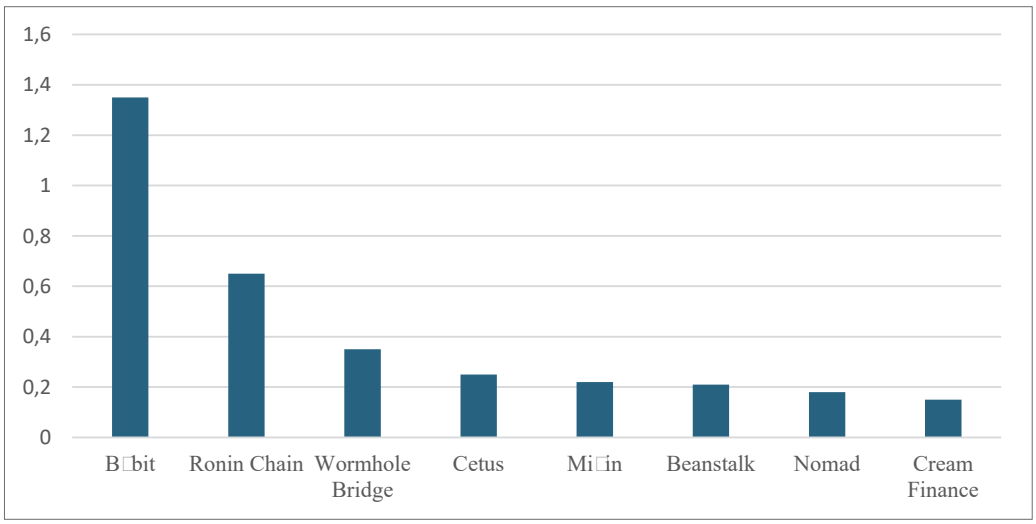

Рис. 3. Найбільші кіберінциденти у DeFi-секторі 2017–2025 рр.
Джерела: [13; 14; 20; 24; 26]

Bybit — компрометація приватних ключів; Ronin Chain — злам мультипідпису з малою кількістю валідаторів; Wormhole і Nomad — уразливості блокчейн-мостів; Mixin, Beanstalk, Cream Finance — комбінації атак типу flash loan та маніпуляцій ораклами. Спільний знаменник — залежність від централізованих компонентів у нібито децентралізованих системах (ефект Fake-DeFi), яка створює «вузькі місця» керування ключами, мультипідписами й ораклами та полегшує каскадне поширення наслідків через мережеві зв'язки протоколів [24].

З позицій кіберекономіки ці інциденти свідчать про формування алгоритмічного ризику поведінки: дії коду стають тригерами ринкових коливань і втрат ліквідності. На відміну від традиційних фінансових криз, у DeFi відсутній «регулятор останньої інстанції», тож локальна помилка одного протоколу здатна запустити ефект доміно через мережеві зв'язки. Звідси випливає потреба у багаторівневій системі кіберстійкості DeFi, що вміє самостійно виявляти, ізолювати й відновлюватися після атак. Це означає перехід від реактивного захисту до превентивного, у якому безпека є частиною логіки смартконтрактів, а моніторинг і реагування — ончейн та автоматизовані [12].

Типологія атак свідчить, що найбільш небезпечні три категорії:

1. Атаки типу flash loan (*flash loans*) — миттєві беззаставні позики для штучного зміщення цін, ліквідності пулів чи запуску ліквідацій, що спричиняє збитки протоколам.

2. Маніпуляції ораклами (*oracle manipulation*) — контроль/підміна джерел даних або алгоритмів передавання цін, унаслідок чого смартконтракти виконують хибні транзакції.

3. Експлойти блокчейн-мостів (*bridge exploits*) — це вразливості в системах, які дозволяють зловмисникам перехоплювати активи або дані під час їхнього переміщення між різними блокчейнами.

Такі механізми атак формують ядро кіберризиків DeFi, поєднуючи технічні вразливості з економічними наслідками у вигляді втрат активів, порушення цілісності даних і зниження довіри; безпека виходить за межі суто програмного захисту й залежить від взаємодії технологічних, поведінкових і ринкових чинників. За даними К. Карпентьє-Дежардена (Carpentier-Desjardins, C.), М. Пакє-Клустона (Paquet-Clouston, M.), С. Кіцлера (Kitzler, S.) та Б. Гаслгофера (Haslhofer, B.) [10], близько 64% інцидентів повторюють відомі патерни; середні збитки на кейс перевищують 10 млн. дол. США, а повертається менш як 20% коштів, що свідчить про низьку постатакувальну стійкість протоколів.

Дані свідчать, що найбільшу загрозу становлять атаки на блокчейн-мости, оскільки вони створюють централізовані точки входу, що суперечить логіці децентралізації. Це узгоджується з результатами О. Агудело (Agudelo, C. S.) [3], який показує, що близько 70% інцидентів зумовлені недосконалістю верифікаційних протоколів підтвердження на блокчейн-мостах. Характерні кейси — Ronin (2022) та Multichain (2023) — спричинили масові втрати користувачів і відтік ліквідності на суміжних ринках TradFi.

Статистичні спостереження підтримують висновок Ф. А. Бакаре (Bakare, F. A.) [8] про перехід DeFi від технологічного експерименту до системно значущого сегмента цифрової економіки: його частка у вартості активів крипторинку у 2024 р. перевищила 25%, що підсилює потенційні макрофінансові наслідки. За результатами моделювання А. М. Огуннолу, О. О. Оланійї та О. М. Огунмолу [22] збої в DeFi можуть безпосередньо впливати на стабільність банків через ланцюги ліквідності та похідні інструменти. Окрема увага приділяється spillover-ефектам між секторами: модель С. Ауф'єро, Ф. Каччолі та П. Віво [7] демонструє двосторонні

Таблиця 1

Основні типи кібератак у DeFi та їхні економічні наслідки, 2017–2024

Тип атаки	Кількість випадків	Частка у загальних втратах	Середні збитки, млн. USD	Приклади протоколів
Flash loans	52	28%	7.2	bZx, PancakeBunny
Oracle manipulation	38	21%	9.8	Mango Markets, Harvest
Bridge exploits	31	33%	15.4	Ronin, Wormhole, Multichain
Governance exploits	12	9%	5.7	Beanstalk, Tornado Cash
Інше	27	9%	2.3	різні DEX-проекти

Джерело: систематизовано автором на основі [10; 13; 20]

зв'язки між DeFi та банківською ліквідністю. У разі атаки на великий DeFi-протокол (наприклад, Curve або Aave) спостерігається перетік ліквідності до CeFi й короткочасні сплески волатильності на фіатних ринках. Це підтверджує системний характер ризиків DeFi і потребу в моделях кіберстійкості, здатних забезпечувати безперервність операцій навіть за локальних збоїв.

У цьому контексті показовими є результати досліджень, які запропонували інноваційні аналітичні платформи для моніторингу транзакцій DeFi на основі машинного аналізу поведінкових аномалій. Такі рішення дозволяють виявляти нетипові шаблони активності користувачів у реальному часі та прогнозувати потенційні збої до моменту їхнього настання. У свою чергу, Д. де Леон (de Leon, J.) [12] довів, що використання алгоритмів навчання з підкріпленням (reinforcement learning, RL) для перевірки смартконтрактів дає змогу на 35–40% знизити частоту критичних помилок. Таким чином, поєднання штучного інтелекту з блокчейн-аналітикою формує нову технологічну основу безпеки.

Узагальнення аналітичних результатів дає змогу стверджувати, що DeFi-сектор сьогодні характеризується трьома ключовими закономірностями:

1) високим рівнем повторюваності атак, що вказує на незрілість механізмів захисту;
2) системними ефектами між секторами фінансового ринку;
3) активною еволюцією кіберзахисних технологій, орієнтованих на штучний інтелект і поведінкову аналітику.

У цифровій економіці DeFi сформувало нову фінансову архітектуру, що виходить за межі класичних моделей посередництва. На відміну від CeFi, DeFi поєднує алгоритмічну автономію з відкритим управлінням, але це породжує феномен асиметричної безпеки — інновації випереджають спроможність системи до самозахисту. DeFi варто трактувати як соціотехнічну систему з гібридною природою ризиків (алгоритмічні, поведінкові, регуляторні). Відбувається зсув довіри від правових норм до коду, що формує парадокс цифрової довіри: більше автономії — менше гарантій стабільності. Це висвітлює методологічну дилему для класичних теорій ризику, які не враховують самонавчальні та взаємозалежні властивості протоколів DeFi [4; 23].

Результати аналізу показують, що ризики DeFi не зводяться до технічних збоїв, а мають системний і поведінковий характер. За висновками С. Ауф'єро (Aufiero, S.) та С. Бартолуччі (Bartolucci, S.) [4], близько 78% втрат мають синергетичну природу — виникають через взаємодію кількох протоколів одночасно. Такі ефекти є продуктом нелінійної динаміки мереж і не охоплюються стандартним аудитом. Це підкреслює обмеженість класичних метрик VaR та CVaR, які імпліцитно припускають наявність централізованого носія ризику. Для децентралізованих

Таблиця 2

Сучасні технологічні підходи до виявлення ризиків у DeFi-протоколах

Метод	Принцип дії	Очікуваний ефект	Приклади застосування
Моніторинг на основі ML	Аналіз поведінкових аномалій транзакцій	Рання ідентифікація шахрайських схем	Chainalysis Reactor, Forta
Аудит на основ RL	Автоматизоване тестування смартконтрактів на вразливості	Підвищення якості коду та зменшення помилок	DeLeon AI Audit Framework
Графовий	Побудова графових зв'язків між адресами	Виявлення взаємозалежних атак	Elliptic, CipherTrace

Джерело: систематизовано автором на основі [10; 13; 20]

систем потрібна метатеорія ризику DeFi, що спирається на принципи мережевої стійкості, кібернетичного зворотного зв'язку та теорії складних систем. У цьому контексті доречним є поняття інституційної вразливості DeFi — системної нездатності децентралізованих структур забезпечити контроль і відповідальність без зовнішнього регулятора.

Децентралізовані фінанси довели, що повна децентралізація не гарантує стійкості й самовідновлення, адже автономні протоколи без централізованого контролю підвищують вразливість до кіберінцидентів. Необхідна кіберстійкість DeFi як інтегрована модель безпеки, що поєднує технологічний, регуляторний і поведінковий виміри. На технологічному рівні йдеться про алгоритмічну безпеку, автоматизований аудит смартконтрактів, застосування штучного інтелекту для виявлення аномалій та системи раннього попередження. Регуляторний вимір передбачає узгодження з MiCA, FATF, DAC8 і CARF для забезпечення прозорості та сумісності без заперечення принципів децентралізації. Поведінковий вимір вимагає культури колективної відповідальності користувачів, розробників і DAO через саморегулювання, етичні норми та цифрову грамотність.

Дослідження Бекемаєра (Bekemeier) [9] та Д. де Леона (de Leon, J.) [12] доводять, що DeFi має еволюціонувати в адаптивні екосистеми самозахисту, здатні автономно передбачати, локалізовувати та нейтралізовувати ризики в реальному часі, тобто перейти від пасивної кібербезпеки до активної кіберстійкості у логіці FinTech 4.0. Запропонована в статті модель кіберстійкості DeFi — це замкнений цикл з чотирьох етапів: ідентифікація, прогнозування, реакція, відновлення.

Етап ідентифікації передбачає постійний моніторинговий шар, який аналізує код смартконтрактів, транзакційні патерни та мережеві зв'язки вузлів, щоб виявляти не лише наявні вразливості, а й системні точки ризику, здатні запускати каскадні збої; таким чином захист переходить із реактивного в превентивний режим і підсилює кіберстійкість. Далі працює прогнозування, де застосування ML і RL разом із графовими нейронними мережами дає

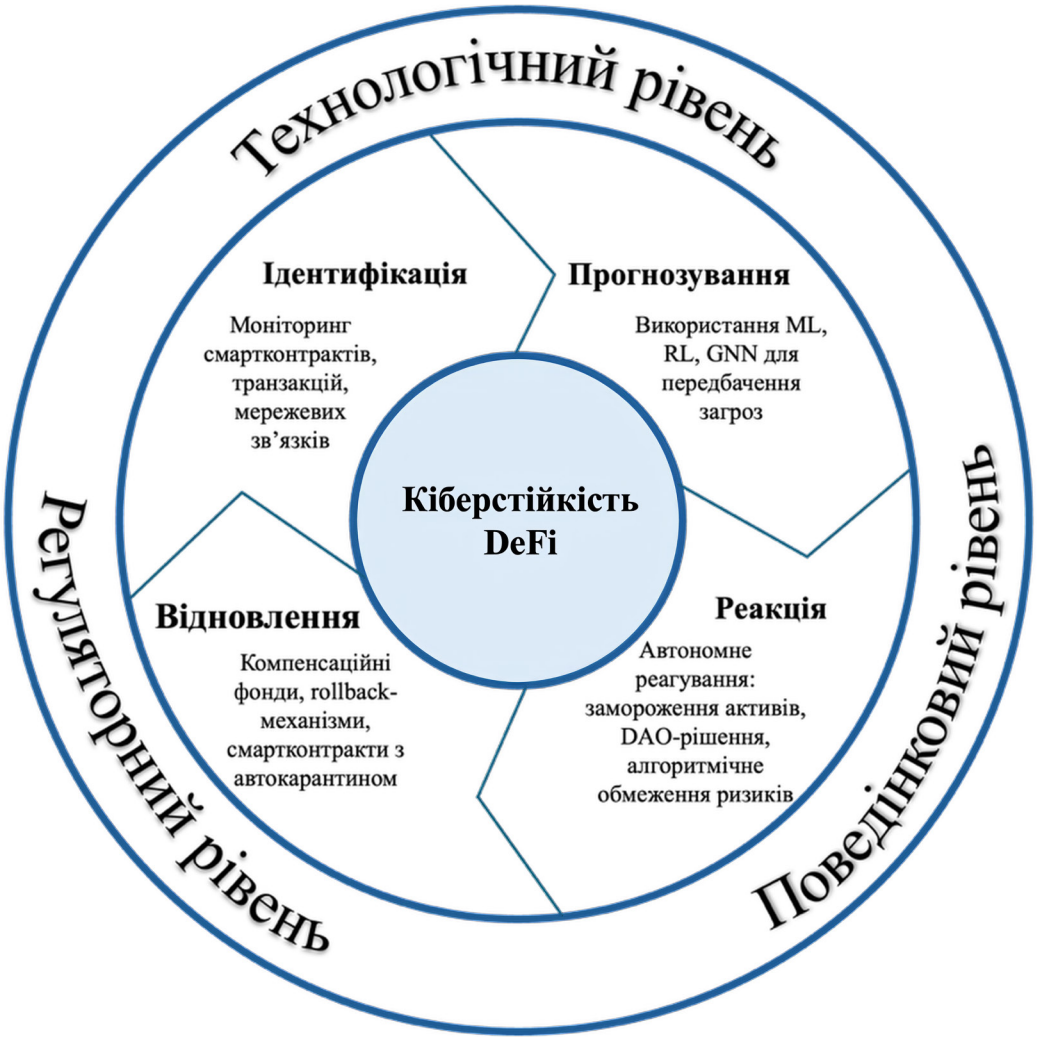

Рис. 4. Концептуальна модель кіберстійкості DeFi
Джерело: запропонована автором

змогу виявляти передумови атак та оцінювати імовірність системних відмов з урахуванням взаємозалежності протоколів, ліквідності та волатильності; на цьому рівні доцільно використовувати інтегральний DeFi Cyber Risk Index (DCRI) як кількісну метрику стану кіберстійкості мережі. Реакція реалізується автономно в коді протоколів через автоматичне замороження активів на підозрілих адресах, колективні рішення DAO щодо відновлення чи блокування операцій та динамічне обмеження ліквідності за ознак аномальної активності, що забезпечує горизонтальний розподіл функцій безпеки і формує середовище саморегульованої відповідальності учасників.

Фінальний етап — відновлення — полягає у створенні механізмів саморегуляції та компенсації. Відновлення відбувається за рахунок DAO-компенсаційних фондів (Decentralized Insurance Pools), які відшкодовують збитки користувачам після колективного голосування, а також rollback-механізмів, що дають змогу повернути стан мережі до попередньої безпечної версії. Інноваційним елементом є смартконтракти з функцією «автокарантину», що тимчасово відключають уражений сегмент до завершення аудиту. Таким чином, DeFi демонструє можливість автономного відновлення без централізованого адміністрування, переходячи від концепції resilience-as-protection до resilience-as-evolution — тобто здатності системи ставати сильнішою після кризових подій.

Узгодження з рамками на кшталт MiCA, DAC8, FATF Travel Rule та CARF відкриває можливість гібридного управління DeFi, у якому технологічна децентралізація поєднується з базовою прозорістю й підзвітністю, але без надмірної централізації контролю; оптимальним інструментом виступає алгоритмічна відповідальність, коли норми безпеки та комплаєнсу кодуються безпосередньо у смартконтракти. Практика окремих юрисдикцій демонструє рух до надання протоколам статусу цифрових суб'єктів і формування децентралізованого правового поля, де виконання правил забезпечується технологічно. На макрорівні ризики DeFi слід трактувати як економічні екстерналії цифрових інновацій: вони породжують соціальні витрати кіберризику — від прямих втрат користувачів і просідання ліквідності до репутаційних збитків і бюджетних витрат на реагування — та здатні трансформуватися у ринкові шоки. Отже, DeFi постає не просто технологією, а складною соціотехнічною екосистемою, чия довгострокова життєздатність залежить від вбудованої кіберстійкості, що забезпечує не лише захист і відновлення, а й еволюційне посилення системи після інцидентів.

Висновки і перспективи подальших досліджень. Децентралізовані фінанси демонструють, що інноваційність не гарантує ані стійкості, ані самовідновлення: вразливості смартконтрактів, маніпуляції ораклами та слабкість блокчейн-мостів здатні перетворювати локальні інциденти на системні шоки з масштабними втратами. Автономність протоколів без централізованого втручання підсилює залежність від якості коду й інфраструктури, тоді як регуляторна невизначеність і брак уніфікованих стандартів ускладнюють інтеграцію з ширшою фінансовою системою; водночас поведінкові чинники спільноти (довіра, участь у DAO, інформаційна дисципліна) визначають глибину збитків і швидкість відновлення. Запропонована в роботі модель кіберстійкості DeFi переходить від фрагментарного реагування до інтегрованого управління ризиками через замкнений цикл «ідентифікація — прогнозування — реакція — відновлення», що узгоджує технологічний, регуляторний і поведінковий рівні. Подальші дослідження доцільно спрямувати на побудову інтегрального індексу кіберризику DCRI, моделювання spillover-ефектів між DeFi і TradFi, стандартизацію автоматизованої реакції смартконтрактів та дизайн DAO-компенсаційних пулів — як основу еволюції DeFi у більш стійку й передбачувану частину глобальної цифрової економіки.

Виконано в рамках науково-дослідної теми «Кібербезпекові та цифрові трансформації економіки країни воєнного часу: боротьба із кіберзлочинами, корупцією та тіньовим сектором» (No д/р 0124U000544), що фінансується за рахунок коштів державного бюджету.

Література

1. Acharya, V. (2025). DeFi Risks and Rewards: Navigating the Decentralized Financial Ecosystem. AMBCrypto. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5147200 (дата звернення: 01.11.2025).

2. Adisa, O., Ilugbusi, B.S., Obi, O.C., Awonuga, K.F., Adelekan, O.A., Asuzu, O.F., & Ndubuisi, N.L. (2024). Decentralized Finance (DeFi) in the U.S. Economy: A Review — Assessing the Rise, Challenges, and Implications of Blockchain-Driven Financial Systems. *World Journal of Advanced Research and Reviews,* 21(01), 2313–2328. https://doi.org/10.30574/wjarr.2024.21.1.0321.

3. Agudelo, C.S. (2025). Decentralised Finance and Cybersecurity: An Analysis of the Legal, Financial, and Technical Risks and Opportunities Associated with the Use of Cryptocurrencies. *ResearchGate.* https://doi.org/10.13140/RG.2.2.11605.69602.

4. Alotaibi, B. (2025). Cybersecurity Attacks and Detection Methods in Web 3.0 Technology: A Review. Sensors, 25(342). *MDPI.* https://doi.org/10.3390/s25020342.

5. Anker-Sørensen, L., & Zetzsche, D. A. (2022). From Centralized to Decentralized Finance — The Issue of "Fake-DeFi". *SSRN*. URL: https://ssrn.com/abstract=3978815 (дата звернення: 01.11.2025).

6. Aramonte, S., Huang, W., & Schrimpf, A. (2021). DeFi risks and the decentralisation illusion. *BIS Quarterly Review*, December 2021, 21–36. https://www.bis.org/publ/qtrpdf/r_qt2112b.htm (дата звернення: 01.11.2025).

7. Aufiero, S., Bartolucci, S., Caccioli, F., & Vivo, P. (2025). Mapping Microscopic and Systemic Risks in TradFi and DeFi: A Literature Review. ResearchGate Preprint. https://doi.org/10.13140/RG.2.2.33979.53287/1.

8. Bakare, F.A., Omojola, J., & Iwuh, A.C. (2024). Blockchain and Decentralized Finance (DeFi): Disrupting Traditional Banking and Financial Systems. *World Journal of Advanced Research and Reviews*, 23(03), 3075–3089. https://doi.org/10.30574/wjarr.2024.23.3.2968.

9. Bekemeier, F. (2021). Deceptive Assurance? A Conceptual View on Systemic Risk in Decentralized Finance (DeFi). *In 2021 4th International Conference on Blockchain Technology and Applications (ICBTA 2021), Xi'an, China. ACM*. https://doi.org/10.1145/3510487.3510499.

10. Carpentier-Desjardins, C., Paquet-Clouston, M., Kitzler, S., & Haslhofer, B. (2025). Mapping the DeFi Crime Landscape: An Evidence-Based Picture. *Journal of Cybersecurity*, 2025. https://doi.org/10.1093/cybsec/tyae029.

11. Carter, N., & Jeng, L. (2021). DeFi Protocol Risks: The Paradox of DeFi. In Regtech, Suptech and Beyond: Innovation and Technology in Financial Services (forthcoming). *SSRN*. URL: https://ssrn.com/abstract=3866699 (дата звернення: 01.11.2025).

12. de Leon, J.J., Zhang, C., Koulouris, C.-S., Medda, F., & Rahul, A. (2025). Smart Contract Security in Decentralized Finance: Enhancing Vulnerability Detection with Reinforcement Learning. *Applied Sciences, 15(2)*. https://doi.org/10.3390/app15201234.

13. Doraisamy, V., Ab Rahman Muton, N., Rasalingam, R. R., & Ab Malik, A. A. (2025). Cybersecurity Challenges and Solutions in the Metaverse: A Critical Review of Threats, Risks, and Technologies. *Compendium by paperASIA, 41(4b)*, 267–276. https://doi.org/10.59953/paperasia.v41i4b.604.

14. Gogol, K., Killer, C., Schlosser, M., Bocek, T., Stiller, B., & Tessone, C. (2024). SoK: Decentralized Finance (DeFi) — Fundamentals, Taxonomy and Risks. *University of Zurich, Switzerland.* https://doi.org/10.48550/arXiv.2404.11281.

15. Jensen, J.R., & Ross, O. (2021). Managing Risk in DeFi: Position Paper. *University of Copenhagen & eToroX Labs.* SSRN. URL: https://ssrn.com/abstract=3745568 (дата звернення: 01.11.2025).

16. Juneja, A., Goswami, S.S., & Mondal, S. (2024). Cyber Security and Digital Economy: Opportunities, Growth and Challenges. *Journal of Technology Innovations and Energy, 3(2*). https://doi.org/10.56556/jtie.v3i2.907.

17. Kaur, S., Singh, S., Gupta, S., & Wats, S. (2023). Risk analysis in decentralized finance (DeFi): A fuzzy-AHP approach. Risk Management, 25(13). https://doi.org/10.1057/s41283-023-00118-0.

18. Liang, H., Xu, L., & Zhao, Y. (2024). Risk Management in Decentralised Finance (DeFi). *ResearchGate.* https://doi.org/10.13140/RG.2.2.12352.10241.

19. Liang, W., Johnson, B., & Edward, E. (2025). Cryptocurrency Exchanges as Gatekeepers: Evaluating AML Risks in DeF). ResearchGate. URL: https://www.researchgate.net/publication/395472893 (дата звернення: 01.11.2025).

20. McKay, J. (2022). DeFi-ing Cyber Attacks: A Statistical Analysis of Cybersecurity Attacks in Decentralized Finance. *DEFYIELD Research Paper, April 27*.

21. Ogunnolu, A.M., Olaniyi, O.O., Obrik-uloh, E., Arigbabu, A.T., & Ogunmolu, O.M. (2025). Cyber Risk Spillovers in Interconnected Financial Ecosystems: Evidence from Traditional Banks and DeFi Oracles. *Journal of Engineering Research and Reports, 25(7),* 1156. https://doi.org/10.9734/jerr/2025/v27i711556.

22. Ogunola, A., Ajayi, O.O., Sonubi, T.O., et al. (2024). The Intersection of Digital Safety and Financial Literacy: Mitigating Financial Risks in the Digital Economy. International Journal of Science and Research Archive, 13(2), 2183. https://doi.org/10.30574/ijsra.2024.13.2.2183.

23. Oosthoek, K. (2020). Flash Crash for Cash: Cyber Threats in Decentralized Finance. Delft University of Technology, Cyber Threat Intelligence Lab, Delft, The Netherlands.

24. Semerenska, V. (2024). Analysis of Major Cyber Attacks on DeFi in 2024 and Countermeasures. *Grundlagen der modernen wissenschaftlichen Forschung, Abschnitt 18, 219–224. Zürich: Logos Verlag.* https://doi.org/10.36074/logos-13.12.2024.046.

25. Weingärtner, T., Fasser, F., Sá da Costa, P.R., & Farkas, W. (2023). Deciphering DeFi: A Comprehensive Analysis and Visualization of Risks in Decentralized Finance. *Journal of Risk and Financial Management, 16(10),* 545. https://doi.org/10.3390/jrfm16100545

26. Werner, A., Dawodu, S., & Kaur, R. (2025). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and Its Applicability to Decentralized Finance (DeFi). *SSRN*. URL: https://ssrn.com/abstract=5133050 (дата звернення: 01.11.2025).