http://www.moderntechno.de/index.php/meit/article/view/meit34-00-036
DOI: 10.30890/2567-5273.2024-34-00-036

УДК 000

CYBER RISKS ON CRYPTOCURRENCY EXCHANGES: CAUSES, CONSEQUENCES, AND THEIR MITIGATION

КІБЕРРИЗИКИ НА КРИПТОВАЛЮТНИХ БІРЖАХ: ПРИЧИНИ, НАСЛІДКИ ТА ЇХ МІНІМІЗАЦІЯ

Hrebelnyi A.B. / Гребельний А.Б.
Kyiv National Economic University n.a. Vadym Hetman, Kyiv, Beresteiskyi Ave. 54/1, 02000
Київський національний економічний університет ім. Вадима Гетьмана, Київ, Берестейський просп. 54/1, 02000

Анотація. *У статті розглядаються кіберризики, які виникають на криптовалютних біржах, їх причини, наслідки та шляхи мінімізації. Аналізуючи реальні випадки атак, ми ідентифікуємо основні типи загроз та пропонуємо рекомендації для зменшення ризиків. Мета дослідження полягає у виявленні закономірностей у виникненні кіберризиків та розробці заходів, які можуть мінімізувати їх вплив на ринок криптовалют. Основні результати включають опис типових атак на біржі, їх наслідків для користувачів та ринку в цілому, а також рекомендації щодо покращення безпеки. Дослідження має практичне значення для подальшого розвитку систем безпеки на криптовалютних біржах.*

Ключові слова: *Кібербезпека, криптовалютні біржі, кіберризики, фішингові атаки, DDoS-атаки, злами гаманців, експлойти, технічні уразливості, організаційні слабкості, контроль доступу, людський фактор, аудит безпеки, холодні гаманці, багатофакторна автентифікація (MFA), моніторинг інцидентів.*

Вступ.

З розвитком криптовалютних технологій зростає і кількість кіберризиків пов'язаних із їх використанням. Криптовалютні біржі, які є основними платформами для торгівлі цифровими активами, стають привабливою мішенню для кіберзлочинців. Відсутність централізованого регулювання та високий ступінь анонімності роблять ці платформи вразливими до різноманітних атак.

Основна проблема полягає в тому, що криптовалютні біржі є привабливою мішенню для хакерів через високий обіг цифрових активів і, часто, недостатній рівень захисту (рис. 1). Атаки на біржі можуть мати серйозні наслідки, включаючи втрату значних обсягів криптовалюти, зниження довіри інвесторів і збитки для економіки в цілому. Такі інциденти, як злам Mt. Gox у 2014 році, Bitfinex у 2016 році, Coincheck у 2018 році та Binance у 2019 році, наштовхують на необхідність глибокого аналізу та розробки ефективних заходів безпеки для захисту криптовалютних бірж. Vasek & Moore, "The significant losses resulting from these incidents underscore the need for robust security measures in cryptocurrency exchanges" значні втрати, спричинені цими інцидентами, визначають необхідність впровадження надійних заходів безпеки на криптовалютних біржах [4].

У цій статті буде проведено дослідження основних причин кіберризиків на криптовалютних біржах, аналіз відомих інцидентів та їх наслідків, а також розробку рекомендацій щодо зменшення цих ризиків. Ми розглянемо основні типи атак, які загрожують криптовалютним біржам та запропонуємо стратегії для покращення безпеки і зниження ризиків фінансових втрат. Як підкреслюють Narayanan, "The need for comprehensive security protocols is

paramount to maintaining the integrity and trustworthiness of cryptocurrency markets" необхідність комплексних протоколів безпеки є надзвичайно важливою для підтримання цілісності та довіри до ринків криптовалют [3].

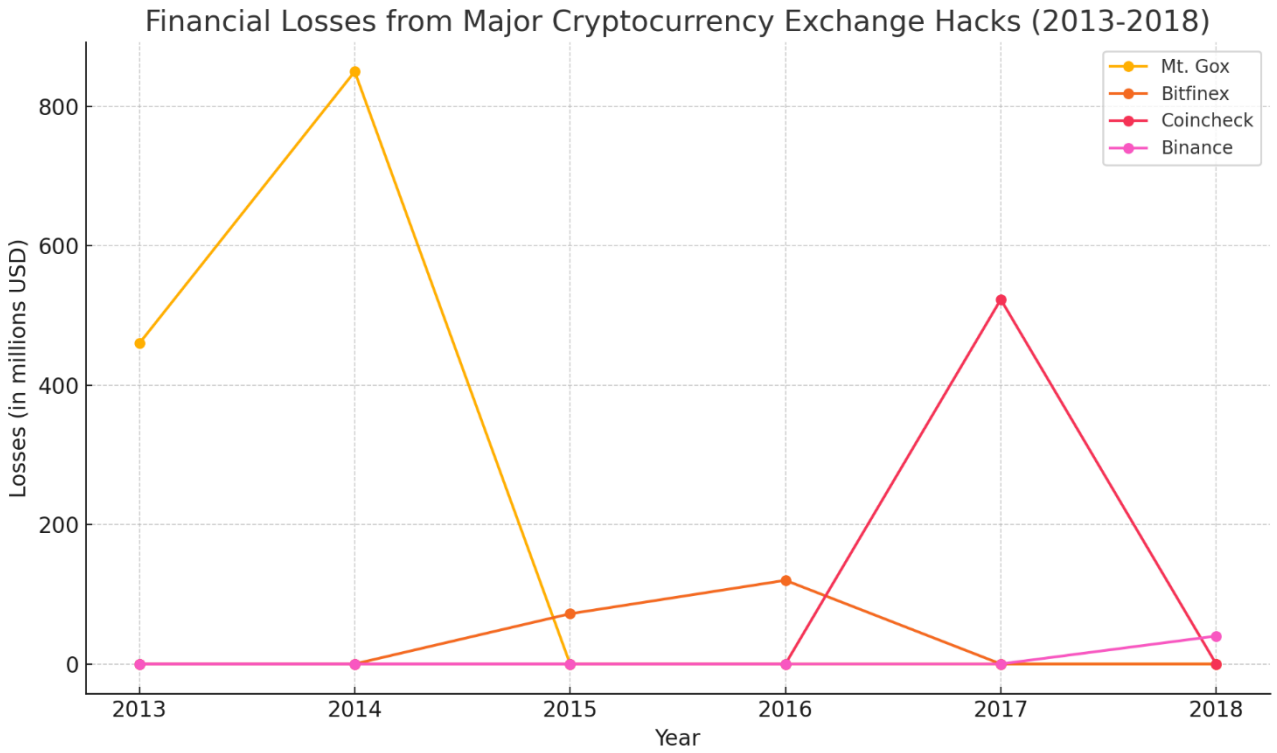

Рис. 1 Діаграма ілюструє фінансові втрати, пов'язані з основними зламами криптовалютних бірж за період з 2013 по 2018 роки, підкреслюючи масштаб проблеми та необхідність впровадження надійних заходів безпеки.

Причини кіберризиків на криптовалютних біржах

Криптовалютні біржі є важливими учасниками фінансової системи, але через свою природу вони вразливі до численних кіберризиків. Основні причини можна класифікувати:

- технічні уразливості,
- організаційні слабкості,
- людський фактор.
- недостатній контроль доступу,

Технічні уразливості є однією з головних причин кіберризиків на криптовалютних біржах. Вони включають вразливості в програмному забезпеченні, які можуть бути використані зловмисниками для доступу до гаманців та викрадення криптовалюти. Скажімо, злам Mt. Gox у 2014 році був спричинений помилкою в коді, що дозволило хакерам викрасти понад 850 000 BTC. Bonneau зазначають, що "The decentralized nature of cryptocurrencies presents unique security challenges that traditional financial systems do not encounter" децентралізований характер криптовалют створює унікальні проблеми безпеки, з якими традиційні фінансові системи не стикаються [4].

Однією з найбільш поширених технічних вразливостей є використання гарячих гаманців для зберігання активів. Гарячі гаманці підключені до

інтернету і тому більш вразливі до атак. Хоча вони зручні для швидкого доступу та торгівлі, їх безпека часто залишається під загрозою. Крім того, багато бірж не проводять регулярні аудити безпеки, що дозволяє зловмисникам знаходити та використовувати вразливості.

Організаційні слабкості також відіграють значну роль у виникненні кіберризиків. Це може включати недостатню увагу до розробки та впровадження політик безпеки, відсутність регулярних перевірок та недостатнє фінансування заходів безпеки. Біржі часто зосереджуються на функціональності та швидкості роботи, що може призводити до ігнорування або недооцінки ризиків безпеки.

Недостатня увага до кадрової політики також може призводити до проблем. Для прикладу, відсутність належного навчання персоналу з питань кібербезпеки може створити слабкі місця, які зловмисники можуть використовувати для здійснення атак.

Крім того, відсутність належного контролю доступу до критично важливих систем може призвести до внутрішніх загроз, коли поточні або колишні співробітники зловживають своїми привілеями.

Типи атак та ризики

Криптовалютні біржі зазнають численних атак, які можуть мати серйозні фінансові та репутаційні наслідки. Основні типи атак включають фішингові атаки, DDoS-атаки, злами гаманців та експлойти в програмному забезпеченні бірж (рис. 2). Розглянемо ці типи атак більш детально.

Фішингові атаки є одним із найпоширеніших та ефективних методів викрадення даних ідентифікації користувачів. Зловмисники створюють підроблені веб-сайти або надсилають електронні листи, що виглядають як справжні повідомлення від біржі, щоб обманом змусити клієнтів розкрити свої логіни та паролі. Згідно з дослідженням, проведеним Vasek & Moore, "Phishing attacks have been remarkably successful in targeting cryptocurrency users, often resulting in substantial financial losses", фішингові атаки показали надзвичайний успіх у використанні проти користувачів криптовалют, де це часто призводило до значних фінансових втрат [4].

Атаки типу "відмова в обслуговуванні" (DDoS) використовуються для тимчасового виведення біржі з ладу. Зловмисники надсилають великий обсяг трафіку на сервери біржі, перевантажуючи їх і роблячи платформу недоступною для користувачів. Хоча такі атаки не часто призводять до безпосередньої утрати активів, вони можуть бути використані для відволікання уваги під час здійснення інших типів атак або для дискредитації біржі.

Злами гаманців є найбільш руйнівними типами атак, оскільки вони призводять до безпосередньої втрати цифрових активів. Злами можуть відбуватися через вразливості в програмному забезпеченні гарячих гаманців, які зберігають активи в онлайн-режимі, або через фізичний доступ до приватних ключів..

Експлойти в програмному забезпеченні бірж включають використання зловмисниками вразливостей у коді платформи. Такі атаки можуть бути дуже складними і вимагають високого рівня технічної експертизи. Інцидент з

Bitfinex у 2016 році, який призвів до втрати 120 000 BTC, був здійснений через вразливість у багатопідписних гаманцях. Цей тип втручання підкреслює важливість регулярного аудиту безпеки та оновлення програмного забезпечення.

Контроль доступу є важливим аспектом безпеки будь-якої структури, і криптовалютні біржі не є винятком. Відсутність належного контролю доступу може дозволити зловмисникам отримати доступ до конфіденційної інформації або механізмів, що управляють грошовими потоками. Narayanan підкреслюють, що "The security of cryptocurrency wallets is critical, and any breach can lead to devastating losses" безпека криптовалютних гаманців є критичною і будь-який злам може призвести до катастрофічних втрат [3].

Багато бірж не використовують багатофакторну автентифікацію для доступу до критичних систем, що значно підвищує ризик несанкціонованого входу. Крім того, відсутність регулярних перевірок та оновлень політик доступу може призвести до того, що старі та неактуальні облікові записи залишаються активними, надаючи зловмисникам можливість для атак.

Людський фактор залишається одним з найбільш непередбачуваних і складних для управління аспектів безпеки. Користувачі та співробітники бірж можуть ненавмисно створити умови для успішної атаки через недбалість, помилки або недостатність знань і досвіду. Фішингові атаки часто базуються на обмані та маніпуляції користувачами, змушуючи їх розкрити свої облікові дані.

Недостатнє навчання користувачів щодо розпізнавання загроз, таких як фішингові електронні листи або підозрілі посилання, може зробити їх легкою мішенню для зловмисників. Зазначимо, відсутність культури безпеки в організації може призвести до того, що співробітники не будуть приділяти належної уваги безпеці своїх дій, створюючи додаткові вразливості.

Для ілюстрації цього наводимо діаграму розподілу основних типів атак на криптовалютні біржі:

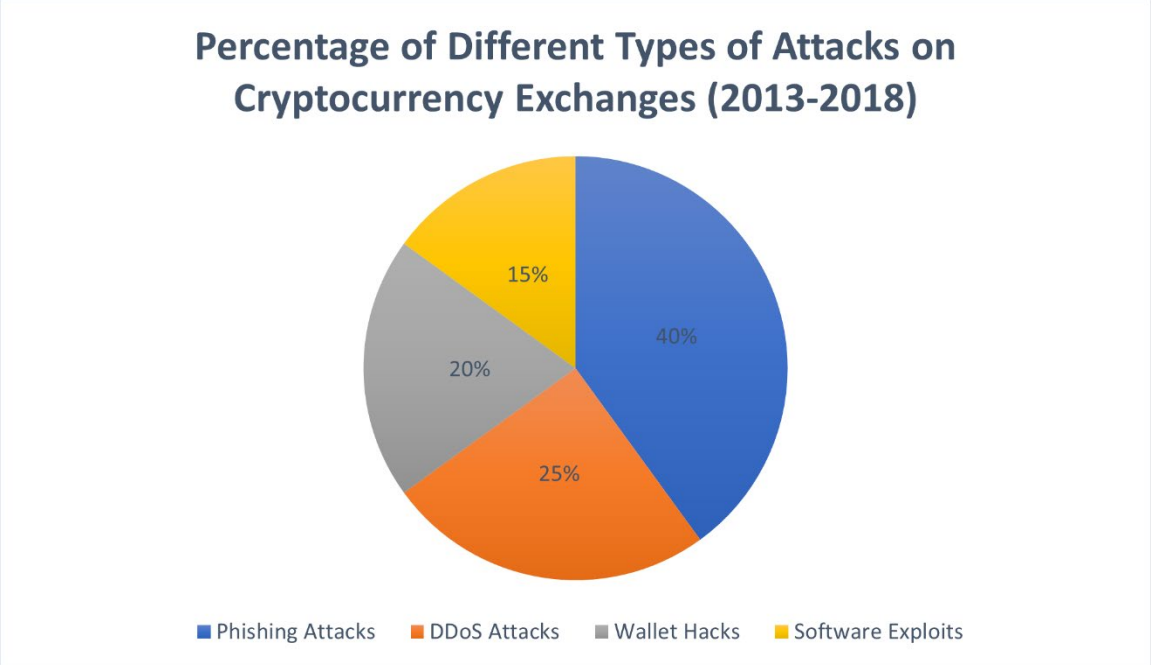

Рис. 2. Відсоток різних типів атак на криптовалютні біржі (2013-2018)

Ця діаграма показує, що фішингові атаки складають найбільшу частку серед усіх атак на криптовалютні біржі. Це підкреслює важливість підвищення обізнаності користувачів та впровадження додаткових заходів безпеки для захисту від цього типу загроз.

Наслідки кібератак

Кібератаки на криптовалютних біржах мають серйозні наслідки, які впливають не тільки на самі біржі, але й на весь ринок криптовалют, їх користувачів та інвесторів.

Фінансові збитки є найбільш очевидним наслідком кібератак на криптовалютні біржі. Злами гаманців та інших структур можуть призвести до втрати значних сум грошей. Злам Mt. Gox у 2014 році та Bitfinex у 2016 році призвів до втрат криптовалюти на сотні мільйонів доларів, що суттєво знизило довіру до платформи та викликало паніку серед інвесторів.

Кібератаки на криптовалютні біржі значно підривають довіру користувачів до цих платформ та ринку криптовалют в цілому. Коли користувачі втрачають свої активи через злами або інші кіберінциденти, вони стають менш схильними до інвестицій та збереження своїх коштів на таких платформах. Це може призвести до відтоку користувачів сервісу.

Часті злами криптовалютних бірж привертають увагу регуляторів та урядів, що призводить до посилення регуляторних вимог. Регулятори можуть запровадити нові правила та стандарти безпеки, яких біржі повинні дотримуватися. Це може збільшити витрати для дотримання вимог та обмежити інновації у цій сфері. Наприклад, після зламів Coincheck та Mt. Gox у Японії, уряд посилив регулювання криптовалютних бірж, запровадивши більш суворі вимоги до безпеки та контролю за діяльністю бірж.

Кібератаки можуть спричинити значні коливання на ринку криптовалют. Втрата великих сум грошей та зниження довіри інвесторів призводять до падіння цін на криптовалюти та зниження капіталізації ринку. Це впливає на всю криптовалютну екосистему, включаючи майнерів, інвесторів, розробників та клієнтів. Приміром, після зламів Mt. Gox та Bitfinex ринок криптовалют зазнав значних коливань, що відобразилося на вартості біткоїна та інших цифрових активах.

Для більш наочного розуміння наведемо діаграму, яка показує вплив основних зламів на вартість біткоїна (Рис.3).

Зведення до мінімуму кіберризиків на криптовалютних біржах є критично важливою гарантією безпеки цифрових активів, забезпечуючи довіру користувачів. Для цього необхідно впроваджувати комплексні заходи безпеки, що охоплюють як технічні, так і організаційні аспекти. Розглянемо деякі з ключових методів мінімізації кіберризиків.

Багатофакторна автентифікація є однією з найефективніших заходів для захисту облікових записів. MFA вимагає від користувачів підтвердження своєї особи за допомогою кількох різних методів, таких як пароль, мобільний додаток або фізичний токен. Це значно ускладнює несанкціонований доступ до облікових записів, навіть якщо зловмисники отримали пароль користувача.

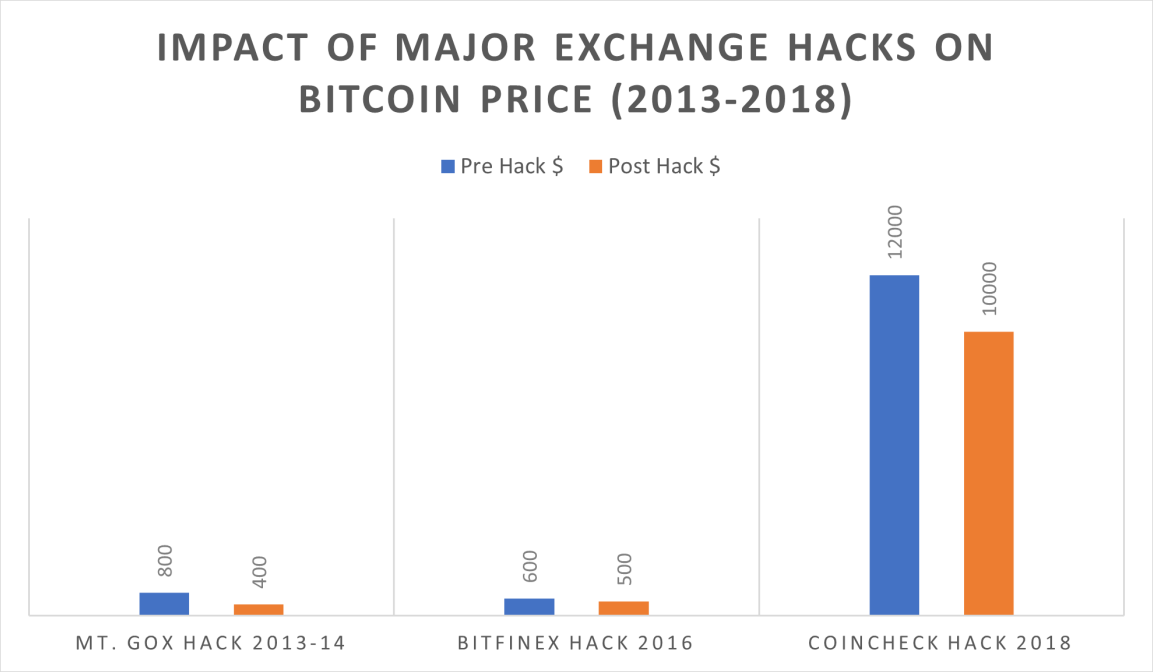

Рис 3. Вплив основних зламів криптовалютних бірж на вартість біткоїна.

Мінімізація кіберризиків

Холодні гаманці зберігають криптовалютні активи в офлайн-режимі, що робить їх недоступними для зламів через інтернет. Біржі можуть використовувати холодні гаманці для зберігання основної частини активів, залишаючи лише невелику кількість в гарячих гаманцях для оперативних потреб. Це значно знижує ризик великих фінансових втрат у випадку зламу гарячих гаманців.

Проведення регулярних аудитів безпеки дозволяє виявляти та ефективно усувати вразливості в програмному забезпеченні та інфраструктурі біржі. Аудити повинні включати перевірку коду, тестування на проникнення та оцінку політик безпеки. Зовнішні аудитори можуть надати незалежну оцінку стану безпеки та запропонувати рекомендації для покращення.

Регулярні оновлення програмного забезпечення є критично важливими для захисту від нових загроз. Розробники постійно випускають оновлення, які виправляють вразливості та покращують безпеку структури. Біржі повинні впроваджувати ці оновлення без затримок, щоб забезпечити максимальний рівень захисту.

Клієнти здебільшого є найслабшою ланкою в системі безпеки. Фішингові атаки та інші методи соціальної інженерії часто спрямовані на обман користувачів та отримання їх облікових даних. Навчання користувачів щодо розпізнавання загроз та коректних практик безпеки може значно знизити ризик успішних атак. Вони повинні знати, як розпізнавати фішингові електронні листи, як безпечно зберігати свої паролі та як використовувати багатофакторну автентифікацію.

Розробка та впровадження чітких протоколів безпеки є основою для захисту біржі. Вони повинні охоплювати всі аспекти безпеки, від контролю доступу до управління інцидентами. Політики безпеки повинні бути регулярно

переглянуті та оновлені відповідно до змін у загрозах та технологіях.

Ефективний моніторинг та швидке реагування на інциденти є ключовими елементами безпеки. Біржі повинні використовувати системи моніторингу для виявлення підозрілої активності та потенційних загроз в режимі реального часу. План реагування на інциденти повинен включати чіткі дії, які необхідно виконати в разі атаки, щоб мінімізувати шкоду та відновити нормальну роботу біржі.

Висновки.

Кіберризики на криптовалютних біржах становлять серйозну загрозу для безпеки цифрових активів і стабільності всього ринку криптовалют. Виявлення та аналіз основних причин, типів атак та наслідків цих ризиків є критично важливими для розробки ефективних заходів захисту. Технічні уразливості, організаційні слабкості, недостатній контроль доступу та людський фактор є основними джерелами кіберризиків. Фішингові атаки, DDoS-атаки, злами гаманців та експлойти в програмному забезпеченні становлять найбільшу загрозу для криптовалютних бірж.

Основні наслідки кібератак включають значні фінансові збитки, зниження довіри користувачів, вплив на ринок криптовалют і викликає паніку серед інвесторів. Часті злами привертають увагу регуляторів, що може спричинити посилення вимог і збільшення обсягу витрат на їх дотримання. Крім того, кібератаки можуть спричинити значні коливання на ринку криптовалют, що впливає на всю криптовалютну систему.

Мінімізація кіберризиків вимагає впровадження комплексних заходів безпеки. Серед них багатофакторна автентифікація, використання холодних гаманців, регулярний аудит безпеки та оновлення програмного забезпечення є критично важливими для забезпечення захисту активів. Навчання користувачів щодо розпізнавання загроз та впровадження чітких політик безпеки допомагають знизити ризики людського фактора. Ефективний моніторинг та швидке реагування на інциденти дозволяють виявляти та усувати загрози, мінімізуючи їх вплив.

Подальші дослідження та розвиток технологій безпеки є необхідними для адаптації до нових загроз та забезпечення надійного захисту криптовалютних бірж. Впровадження передових методів шифрування, автоматизованих систем моніторингу та штучного інтелекту може значно покращити захист від кіберзагроз. Співпраця між біржами, регуляторами та дослідницькими інститутами є важливою для розробки ефективних стратегій захисту та обміну інформацією про нові загрози.

Таким чином, забезпечення кібербезпеки криптовалютних бірж є складним і багаторівневим завданням, яке потребує постійного вдосконалення. Комплексний підхід до мінімізації ризиків, що включає технічні, організаційні та освітні заходи, є ключовим для створення безпечного та надійного середовища для торгівлі цифровими активами.

Література:

1. Юрій Когут "Технології блокчейн та криптовалюта: ризики та

кібербезпека" Сідкон, Київ, 2022.

2. Conti, M., E, S. K., Lal, C., & Ruj, S. "A survey on security and privacy issues of Bitcoin." IEEE Communications Surveys & Tutorials, 2018.

3. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies." IEEE Symposium on Security and Privacy, 2015.

4. Vasek, M., & Moore, T. "There's no free lunch, even using bitcoin: Tracking the popularity and profits of virtual currency scams." Financial Cryptography and Data Security, Springer, Berlin, Heidelberg, 2015.

Abstract. *This article addresses the cyber risks associated with cryptocurrency exchanges, their causes, consequences, and mitigation strategies. By analyzing real attack incidents, we identify the main types of threats and propose recommendations to reduce these risks. The study begins with an overview of the development of cryptocurrency technologies and the increasing number of cyber risks. It then delves into the causes of these risks, focusing on technical vulnerabilities, organizational weaknesses, insufficient access control, and human factors. The article continues with a detailed examination of the different types of attacks on cryptocurrency exchanges, including phishing attacks, DDoS attacks, wallet hacks, and software exploits.*

The consequences of these cyberattacks are explored, highlighting financial losses, decreased user trust, regulatory repercussions, and market impact. The article also discusses strategies for minimizing cyber risks, emphasizing the importance of multifactor authentication, the use of cold wallets, regular security audits, software updates, user training, the implementation of security policies, and effective incident monitoring and response.

Finally, the conclusion summarizes the key findings and underscores the necessity for ongoing research and the development of advanced security technologies to protect cryptocurrency exchanges.

Key words: *Cybersecurity, cryptocurrency exchanges, cyber risks, phishing attacks, DDoS attacks, wallet hacks, exploits, technical vulnerabilities, organizational weaknesses, access control, human factor, security audit, cold wallets, multifactor authentication (MFA), incident monitoring.*

Стаття відравлена: 19.08.2024 р.