МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

15.01. – КМР.1851. – С 2022.12.15.14. ПЗ

СВИРИДЧЕНКА МИКИТИ СЕРГІЙОВИЧА

2023

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

УДК 004.942:336.743

ПОГОДЖЕНО
Декан факультету
інформаційних технологій
д.п.н..
проф _____О.Г.Глазунова
«__»_____ 2023 р

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ
Завідувач кафедри
економічної кібернетики
к.е.н.,
доц._____Володимир Харченко
«__»_____ 2023 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

Моделювання стратегії захисту криптовалютних активів

Спеціальність 051 – «Економіка»
Освітня програма «Економічна кібернетика»
Програма підготовки освітньо-професійна

Гарант освітньої програми: _____ Н.В.Попрозман
підпис

Виконав: _____ М.С.Свиридченко
підпис

Керівник магістерської кваліфікаційної роботи:

_____ Д.М. Жерліцин
підпис

КИЇВ – 2023

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Завідувач кафедри
економічної кібернетики

Проф_____ Д.М.Жерліцин
підпис
"___" _____ 2022 р.

ЗАВДАННЯ
до виконання магістерської кваліфікаційної роботи
студентці Рахнянський Дмитро Сергійович

Спеціальність 051 «Економіка»
Освітня програма «Економічна кібернетика»
Програма підготовки освітньо-професійна

1. Тема роботи: «Моделювання стратегії захисту криптовалютних активів»
Затверджена наказом ректора від 15.12.2022 р. № 1851 «С»

2. Термін подання завершеної роботи на кафедру – 05.11.2023 р.

3. Вихідні дані до роботи (проекту)

4. Перелік графічного матеріалу: 7 малюнків, 3 таблиць.

5. Зміст пояснювальної записки (перелік питань, що підлягають дослідженню в роботі):

a) дати характеристику технології блокчейн як основі функціонування криптовалют;
b) визначити проблеми та перспективу розвитку ринку криптовалютюних активів;
c) проаналізувати концептуальні засади моделювання стратегії захисту криптовалютних активів;
d) дослідити технологічні аспекти захисту криптовалютних активів;
e) охарактеризувати ринкові та соціально-психологічні методи захисту криптовалютних активів;
f) розглянути методи прогнозування ризиків на ринку криптовалютних активів;

g) дати оцінку ефективності існуючих стратегій захисту криптовалютних активів;
h) дослідити оптимізаційну (імітаційну) модель стратегії захисту криптовалютних активів - постановка задачі та її розв’язок;
i) визначити перспективи розвитку ринку криптовалютних активів з урахуванням розроблених стратегій їх захисту.

6.Дата отримання завдання – 15.12.2022р.

Керівник магістерської кваліфікаційної роботи д.е.н., проф. _____ Д.М. Жерліцин
Завдання прийняв до виконання _____ М.С. Свиридченко

РЕФЕРАТ

Тема: «Моделювання стратегії захисту криптовалютних активів»

Магістерська кваліфікаційна робота викладена на 96 сторінках комп'ютерного тексту, містить 3 таблиць, 7 рисунків. Робота складається із вступу, трьох розділів, висновків та списку використаних джерел із 50 найменувань.

Об'єктом дослідження є процеси моделювання стратегій захисту, які дозволяють забезпечити конфіденційність, цілісність та доступність криптовалютних активів у відповідності до сучасних вимог кібербезпеки.

Предметом дослідження є механізми моделювання стратегій захисту криптовалютних активів.

Метою роботи є розробка та апробація ефективних моделей стратегій захисту криптовалютних активів, спрямованих на зменшення ризиків кіберзагроз та максимізацію безпеки та надійності цифрових фінансових активів.

Завдання дослідження:

- дати характеристику технології блокчейн як основі функціонування криптовалют;

- визначити проблеми та перспективу розвитку ринку криптовалютюних активів;

- проаналізувати концептуальні засади моделювання стратегії захисту криптовалютних активів;

- дослідити технологічні аспекти захисту криптовалютних активів;

- охарактеризувати ринкові та соціально-психологічні методи захисту криптовалютних активів;

- розглянути методи прогнозування ризиків на ринку криптовалютних активів;

- дати оцінку ефективності існуючих стратегій захисту криптовалютних активів;

- дослідити оптимізаційну (імітаційну) модель стратегії захисту криптовалютних активів - постановка задачі та її розв’язок;

- визначити перспективи розвитку ринку криптовалютних активів з урахуванням розроблених стратегій їх захисту.

Методи дослідження, що використовуються у даній магістерській роботі, базуються на комплексному аналізі інноваційних підходів до захисту криптовалютних активів. Зокрема, використовується аналіз сучасних технічних засобів захисту, вивчення криптографічних протоколів та методів аутентифікації.

Результати дослідження. Магістерська робота є комплексним дослідженням, спрямованим на розробку та моделювання стратегії захисту криптовалютних активів. У роботі були розглянуті та проаналізовані ключові аспекти, що визначають безпеку цих активів, включаючи технологічні, ринкові та соціально-психологічні аспекти.

У розділі 1 роботи було детально досліджено технологію блокчейн, яка є основою для функціонування криптовалют, а також проаналізовано проблеми та перспективи розвитку ринку криптовалютних активів. Визначено концептуальні засади моделювання стратегії захисту криптовалют, які враховують специфіку цих активів.

У другому розділі вивчено технологічні аспекти захисту, ринкові та соціально-психологічні методи захисту криптовалютних активів, а також розглянуто методи прогнозування ризиків на ринку. Цей розділ сприяв розумінню комплексності взаємодії різних аспектів захисту.

Розділ 3, присвячений стратегії захисту гаманців, включає оцінку ефективності існуючих стратегій, розробку оптимізаційної (імітаційної) моделі та розгляд перспектив розвитку ринку криптовалют з урахуванням розроблених стратегій захисту.

У висновках можна підкреслити, що розвиток ринку криптовалют потребує не лише новаторських підходів у використанні технологій блокчейн, але й ефективних стратегій захисту. Отримані результати свідчать про те, що комплексний підхід, який об'єднує технічні та соціальні аспекти захисту, може забезпечити стійкість та безпеку криптовалютних активів у змінному середовищі.

Дана магістерська робота може слугувати підґрунтям для подальших досліджень у сфері кібербезпеки криптовалютних ринків та розробки нових стратегій захисту. Завдяки врахуванню різних аспектів, вона може бути використана як орієнтир для розробників політики безпеки, а також для компаній та індивідуальних користувачів, які працюють з криптовалютними активами.

В контексті швидкого розвитку технологій та поширення криптовалют як альтернативних фінансових інструментів, важливість забезпечення найвищого рівня безпеки для користувачів і їхніх криптовалютних активів надто важлива. Розглядаючи результати досліджень, можна виділити кілька перспектив та висновків, які визначать майбутній розвиток ринку криптовалют:

1. Досягнення максимальної ефективності в захисті криптовалют вимагає інтеграції технічних заходів з соціальними стратегіями. Оптимальне поєднання технічних аспектів (шифрування, систем виявлення вторгнень) і соціальних методів (освіта користувачів, підвищення кібергігієни) сприятиме створенню найбільш надійної системи захисту.

2. Використання імітаційних моделей, як розглядається в розділі 3, може слугувати ефективним інструментом для оптимізації стратегій захисту. Моделювання різних сценаріїв дозволяє оцінити ефективність стратегій у віртуальному середовищі перед їхнім впровадженням в реальному житті.

3. Розробка та уніфікація стандартів безпеки на міжнародному рівні стане ключовим чинником для створення стабільного криптовалютного ринку.

Регулятори мають активну роль у формуванні норм та правил, які забезпечать безпеку та довіру учасників ринку.

4. Розвиток нових технологій, таких як розширені блокчейн-рішення, та їхня адаптація в системах криптовалют створюють нові можливості, але й виклики для безпеки. Інновації в галузі захисту повинні швидко адаптуватися до змін технологічного ландшафту.

5. Посилення заходів безпеки може впливати на соціоекономічні аспекти ринку криптовалют. Довіра інвесторів, легітимність торгових платформ та реакція регуляторів - всі ці фактори важливі для довгострокового стабільного розвитку ринку.

У цілому, враховуючи зазначені перспективи, важливо продовжувати наукові та практичні дослідження в області кібербезпеки криптовалют. Це допоможе створити розвинуті та ефективні стратегії захисту, що відповідають найновішим викликам і можливостям цього унікального ринку.

Ключові слова: криптовалюта, блокчейн, криптобіржі, кіберзпека, захист криптовалют, прозорість операцій, види кібератак, ризик.

АНОТАЦІЯ

Свиридченко М.С. – Моделювання стратегії захисту криптовалютних активів. – Магістерська кваліфікаційна робота.

Магістерська кваліфікаційна робота на здобуття наукового ступеня магістра за спеціальністю 051 «Економіка», освітньою професійною програмою «Економічна кібернетика» – Національний університет біоресурсів і природокористування України Міністерства освіти і науки України, 2023.

У магістерській кваліфікаційній роботі досліджено теоретичні та практичні аспекти стратегій захисту криптовалютних активів. Проведена оцінка сучасного стану методів та засобів кіберзахисту криптовалют. Проаналізовано загрози та ризики, які ставлять під загрозу ці цифрові активи. Запропоновано конкретні стратегії та рекомендації щодо підвищення безпеки криптовалютних операцій та збереження активів в умовах постійно змінюючогося кіберсередовища.

Ключові слова: криптовалюта, блокчейн, криптобіржі, кіберзпека, захист криптовалют, прозорість операцій, види кібератак, ризик.

SUMMARY

Svyrydchenko M.S. – Modeling the strategy of cryptocyrrency assets protection. – Master's qualification work.

Master's qualification thesis for obtaining a master's degree in specialty 051 "Economics", educational professional program "Economic Cybernetics" - National University of Bioresources and Nature Management of Ukraine of the Ministry of Education and Science of Ukraine, 2023.

The thesis examines the theoretical and practical aspects of cryptocurrency asset protection strategies. An assessment of the current state of cybersecurity methods and tools for cryptocurrencies has been conducted. The threats and risks to these digital assets are analyzed. Specific strategies and recommendations are proposed to improve the security of cryptocurrency transactions and preserve assets in an ever-changing cyber environment.

Keywords: cryptocurrency, blockchain, crypto exchanges, cybersecurity, cryptocurrency protection, transparency of operations, types of cyberattacks, risk.

ПЛАН

ВСТУП

Сучасний етап розвитку фінансової сфери характеризується широким використанням криптовалют як важливого інструменту інвестування та зберігання активів. Зростання популярності цифрових валют та їх значущий вплив на світову економіку викликають необхідність створення ефективних стратегій захисту криптовалютних активів в умовах постійної кіберзагрози.

Незважаючи на значущі переваги криптовалют, такі як децентралізація та швидкі транзакції, цей ринок став об'єктом поглибленого вивчення у зв'язку з високим рівнем кіберзагроз та ризиків, пов'язаних із втратою активів через хакерські атаки та інші загрози кібербезпеки.

Дослідженням питань розвитку індустрії криптовалют займаються багато науковців та практиків. Питання сутності криптовалют та тенденції їх розвитку в Україні розглядалося, такими вченими, як Є. О. Галушка [1], І. І Гусєва [2], О. С. Новак, О. М. Петрук [3]. Яцик Т. [4] пропонує розглядати криптовалюту як особливий електронний платіжний засіб, курс якого підтримується тільки попитом і пропозицією, але А. Кувшинова [5] спростувала визначення економічної сутності криптовалюти як грошових коштів, валюти, валютної цінності, електронних грошей тощо. Теоретико-методичні засади обліку, оподаткування та визначення правового статусу операцій з криптовалютами розглянуто в роботах В. М. Костюченко [6], Н. М. Жидовська [7] та І. Спільник [8]. А такі вчені, як І. Самоходський та О. Шелест [9] визначили перелік етапів з яких складається діяльність суб’єктів господарювання на ринку криптовалют. Лук’янчук Р. В. визначає сучасні виклики, пов’язані із розвитком криптоіндустрії [10]. Ширінян Л. В., Роганова Г. О., Ширінян А. С. аналізують фактори, що впливають на вартість біткоїна, серед яких: інші криптовалюти, фіатні гроші, світові показники фондових ринків, акції потужних світових компаній, ціни на енергоресурси, вартість дорогоцінних металів [11]. Отже, незважаючи на значний внесок вчених

недостатньо уваги приділено основним викликам розвитку індустрії криптовалют та визначенню факторів, що впливають на курс криптовалют.

Об'єктом дослідження є процеси моделювання стратегій захисту, які дозволяють забезпечити конфіденційність, цілісність та доступність криптовалютних активів у відповідності до сучасних вимог кібербезпеки.

Предметом дослідження є механізми моделювання стратегій захисту криптовалютних активів.

Метою даного дослідження є розробка та апробація ефективних моделей стратегій захисту криптовалютних активів, спрямованих на зменшення ризиків кіберзагроз та максимізацію безпеки та надійності цифрових фінансових активів. Результати цього дослідження мають потенційно значущі наслідки для розвитку сучасного криптовалютного ринку та підвищення рівня довіри користувачів до цифрових активів.

Завдання дослідження:

- дати характеристику технології блокчейн як основі функціонування криптовалют;

- визначити проблеми та перспективу розвитку ринку криптовалютюних активів;

- проаналізувати концептуальні засади моделювання стратегії захисту криптовалютних активів;

- дослідити технологічні аспекти захисту криптовалютних активів;

- охарактеризувати ринкові та соціально-психологічні методи захисту криптовалютних активів;

- розглянути методи прогнозування ризиків на ринку криптовалютних активів;

- дати оцінку ефективності існуючих стратегій захисту криптовалютних активів;

- дослідити оптимізаційну (імітаційну) модель стратегії захисту криптовалютних активів - постановка задачі та її розв'язок;

- визначити перспективи розвитку ринку криптовалютних активів з урахуванням розроблених стратегій їх захисту.

Методи дослідження, що використовуються у даній магістерській роботі, базуються на комплексному аналізі інноваційних підходів до захисту криптовалютних активів. Зокрема, використовується аналіз сучасних технічних засобів захисту, вивчення криптографічних протоколів та методів аутентифікації.

Наукова новизна роботи полягає в тому, що вона спрямована на розробку та вдосконалення стратегій захисту, які спеціально адаптовані для унікальних характеристик криптовалютних активів. Дослідник враховує не лише технічні аспекти, але й соціально-економічні фактори, які впливають на безпеку цифрових фінансових активів.

Теоретична значущість полягає у розширенні розуміння принципів та методів захисту криптовалют в контексті сучасних тенденцій в галузі кібербезпеки. Автор використовує теоретичні концепції кібербезпеки та криптографії для створення нових стратегій захисту, що враховують особливості криптовалютного середовища.

Практична значущість полягає в тому, що результати дослідження можуть бути використані для розробки практичних рекомендацій та стратегій безпеки для учасників криптовалютного ринку, таких як криптовалютні біржі, інвестори та інші учасники цього екосистеми. Робота дозволить вдосконалити існуючі методи захисту та сприятиме підвищенню рівня кібербезпеки в галузі криптовалют.

Ключові слова: криптовалюта, блокчейн, криптобіржі, кіберзпека, захист криптовалют, прозорість операцій, види кібератак, ризик.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ПРОБЛЕМ ТА РОЗРОБКИ СТРАТЕГІЇ ЗАХИСТУ КРИПТОВАЛЮТНИХ АКТИВІВ

1.1. Технологія блокчейн як основа функціонування криптовалют

Насамперед, слід дати визначення поняттю «криптовалюта».

Криптовалюта – набір концептів та технологій, що спільно утворюють основу для екосистеми цифрових грошей. Грошові одиниці, наприклад, біткоїни використовують для збереження та передачі вартості між учасниками мережі. Саме таке трактування електронної валюти викладено у книзі А. Антонопулоса «Mastering Bitcoin» [1].

Якщо постаратися дати визначення криптовалюті, висловившись більш зрозумілою мовою, можна трактувати це явище як віртуальні гроші, що являють собою криптографічні коди і не мають жодного матеріального аналога. Це ще раз підтверджує те, що криптовалюта не є тими грошима, що виникають у свідомості людини. Є ряд разючих відмінностей, які варто розглянути:

1) цифрові гроші повністю віртуальні та нічим не забезпечені, протилежно долару, в основі якого спочатку лежить золото. Хоча деякі фахівці вважають, що вартість криптовалют визначає кількість витраченої з їхньої виробництво енергії (виключенням є централізовані стейблкоіни (USDT,USDD));

2) всі операції абсолютно анонімні у тому, що система повністю прозора. Сторонній користувач може будь-якої миті переглянути ланцюжок транзакцій, що здійснюються з монетою, але особи, які їх вчинили, будуть заховані за конфіденційними публічними ключами;

3) платіж неможливо скасувати. Дана властивість криптовалюти є одним із ключових. З цього приводу С. Накамото писав: «Відсутність незворотних транзакцій збільшує вартість сервісів, чиї послуги є

невідмінними. Оскільки платіж можна анулювати, продавець мусить бути настороже, вимагаючи від покупця більше інформації, ніж у принципі необхідно»;

4) найважливіша відмінність, з якої, по суті, все почалося, криптовалюта не має єдиного центру управління. Це досягається за рахунок передачі найважливішої функції ведення облікових регістрів від централізованих фінансових установ до мережі автономних комп'ютерів.

Цікаво, що поняття «біткоїн» з’явилося першим, і лише кілька років по тому видання «Forbes» надрукували статтю, після чого термін «криптовалюта» став більш звичним у нашому суспільстві. Зв'язки з тим, що найчастіше биткоїн і криптовалюта ототожнюються, а також біткоїн є першою криптовалютою, що не провалилася, історія виникнення феномену криптоактивів буде розглянута саме з створення електронної монети.

Існує думка, що біткоїн з'явився саме тоді, коли його потребували найбільше. Справді, перша згадка про цю монету спливло поверх попелища чинної банківської системи після низки обвалів на Уоллстріт. Початок довгого шляху криптовалюти стався 31 жовтня 2008 року, коли ще невідомий на той момент програміст С. Накамото виклав у мережу свою статтю "Peer-to-Peer Electronic Cash System". У роботі описується система онлайнового обміну, що включає шифрування та дозволяє двом сторонам обмінюватися одиницями вартості, розголошуючи приватну інформацію про себе та свої фінансові рахунки. Ця система призначена для роботи поза традиційними банківськими структурами та дозволяє учасникам угоди пересилати цифрові гроші безпосередньо один одному – концепція торгівлі без посередників, відома під назвою «рівний рівному». Зникає необхідність у банках чи компаніях, що емітують кредитні картки. В обміні не беруть участь жодні оператори платежів чи інші довірені треті сторони. По суті, це одна із форм цифрової готівки.

Незважаючи на перспективність пропозицій С. Накомото, біткоїн був зустрінений суспільством вкрай скептично. Для цього була низка причин, адже це була далеко не перша спроба створення такої системи. До С. Накамото

подібними технологіями займалися учасники руху шифропанків – вільної асоціації технічних спеціалістів-активістів. Багато вчених прагнули створити анонімну цифрову систему грошового обміну, але як би близько вони не підходили до вирішення цього завдання, ні одні з них не досягли успіху. Проте у системи С. Накамото було кілька унікальних особливостей: грошовим стимулюванням та блокчейном для власників різних комп'ютерів у одній мережі на його підтримку [3].

Методом спроб і помилок С. Накамото та його послідовникам вдалося побудувати систему такою, якою ми її знаємо зараз. Хоча була і низка кризових моментів. Найгіршим роком у розвитку криптовалют визнано вважати 2014 рік. Насамперед, це пов'язано з майже крахом даної грошової одиниці через падіння біржі Mt.Gox. У цей період лише за пару днів знизилася в кілька раз, а також почалася низка публікацій про те, що біткоїн використовується в незаконних цілях для покупки зброї та наркотиків. Проте біткоїн зміг відновитися. До початку 2016 року він коштував 450 доларів, а до листопада вже 740. На сьогоднішній день при черговому обвалу ринку цифрової валюти біткоїн тримає планку ціни на рівні 30 тисяч доларів. З'явилося понад 3000 нових криптовалют з ідентичною технічною основою, але не одна з них за вартістю ще не досягла і вже навряд чи пережене біткоїн.

Динаміка цін на біткоїн за 2021/2022 рік представлено на рисунку 1.

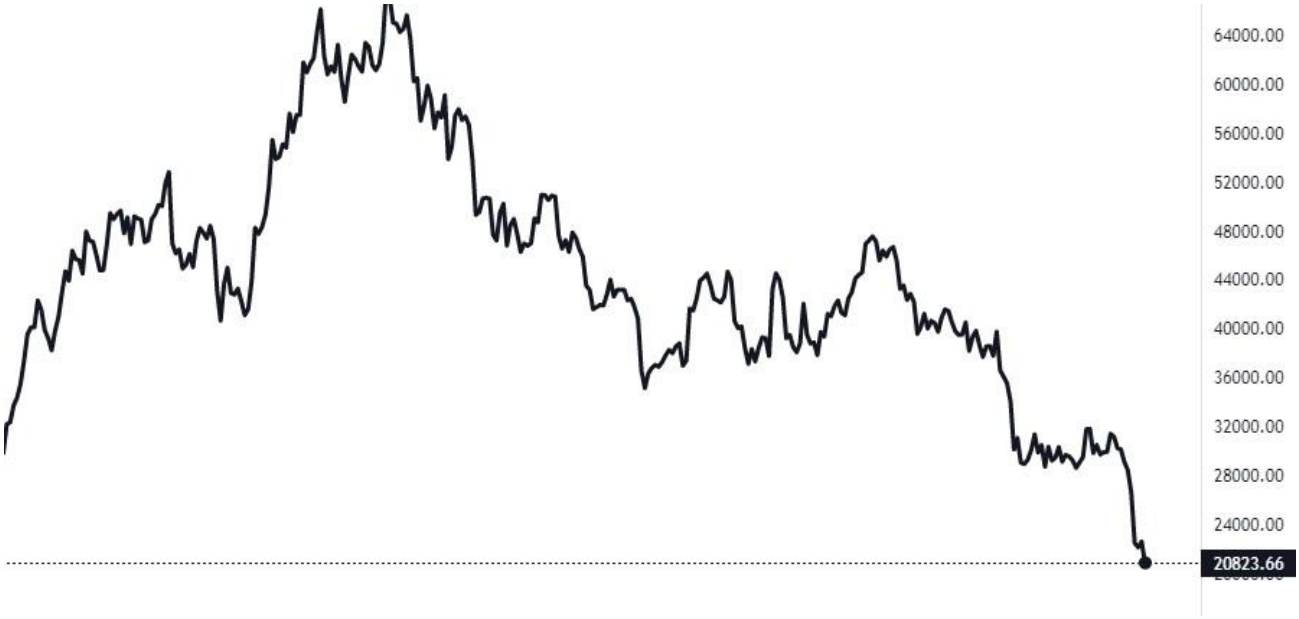

Рисунок 1 – Динаміка цін на біткоїн на 2021/2022 рік [5]

Таким чином, можна зробити висновок, що С. Накамото не є першовідкривачем у сфері криптовалют, і при цьому творець біткоїну невідомий і досі. Сучасні криптоактиви пройшли довгий шлях модернізацій та доробок, що дозволило їм досягти нинішнього становища. Проте явно простежується, що з часом цей вид валюти не стає стійкішим.

Принцип роботи та внутрішня складова являються дуже цікавими особливостями вивчення криптовалюти. Це не буде здаватися складним якщо ми подивимося на це зі сторони теорії Євгена Брікмана. Ще у 19 столітті на полуострові «Яп» так звані камені фей використовувалися для запису та контролю боргів, проте зі збільшенням населення племені ставало важко встежити, хто кому і скільки повинен. Через це виникала напруга у суспільстві, тому старійшини призначали відповідального за контролем записів про всі фінансові звіти пов'язані із камінням фей. Проте ця система не спрацювала, тому що контролери стали стягували процент за ведення кожної виплати або кредиту, а старійшини починали тиснути на них і змушували вносити хибну інформацію. Тож через такі обставини більша частина племені не захотіла централізованого запису боргів, а кожен хто укладав угоду, інформував про це

інших жителів. Тільки якщо більшість погоджувалися з нею, угода вважалася дійсною [2].

Отже, блокчейн є базою криптовалюти та своєрідною обліковою книгою. Можна сказати, блокчейн - це ланцюг із транзакцій, що виробляються в один і той же самий час. Та цей ланцюг буде зростати необмежено довго – стільки, скільки функціонуватиме сама система. Створюючи послідовність перерахувань з фіксацією часу кожного їх, система контролює стан рахунку учасника , та індентифікує прикріплену до біткоїну інформацію, тому, коли він був змайнен, отриман чи витрачен. Блок не зберігається тільки на одному представнику, тому що він існує у великій системі комп'ютерів або мережевих вузлів, які є пристроями на які встановлені електронні гаманці. Якщо казати простіше то це програми які дають користувачам їх паролі та доступ у цілому. Саме використовуючи їх здійснюють управління рахунками користувачів. Мережні вузли працюють разом, і це забезпечує зміст головної журнальної частини, зберігаючи захищеність. Це й робить цю технологію настільки надійною.

Також за його допомогою встановлюють відносини довіри та ідентифікацію особистості, так як ніхто не зможе змінити ланцюг блоків без належних ключів. Що цікаво, блокчейн досить універсальний. А. Тапскотт та Д. Тапскотт, творці «Революції блокчейну» писали: «Це вічний цифровий розподілений журнал економічних транзакцій, який може бути запрограмований не тільки для запису фінансових операцій, а й практично всього, що має цінність» [14].

Схематично принцип роботи блокчейна зображено на рисунку 2.

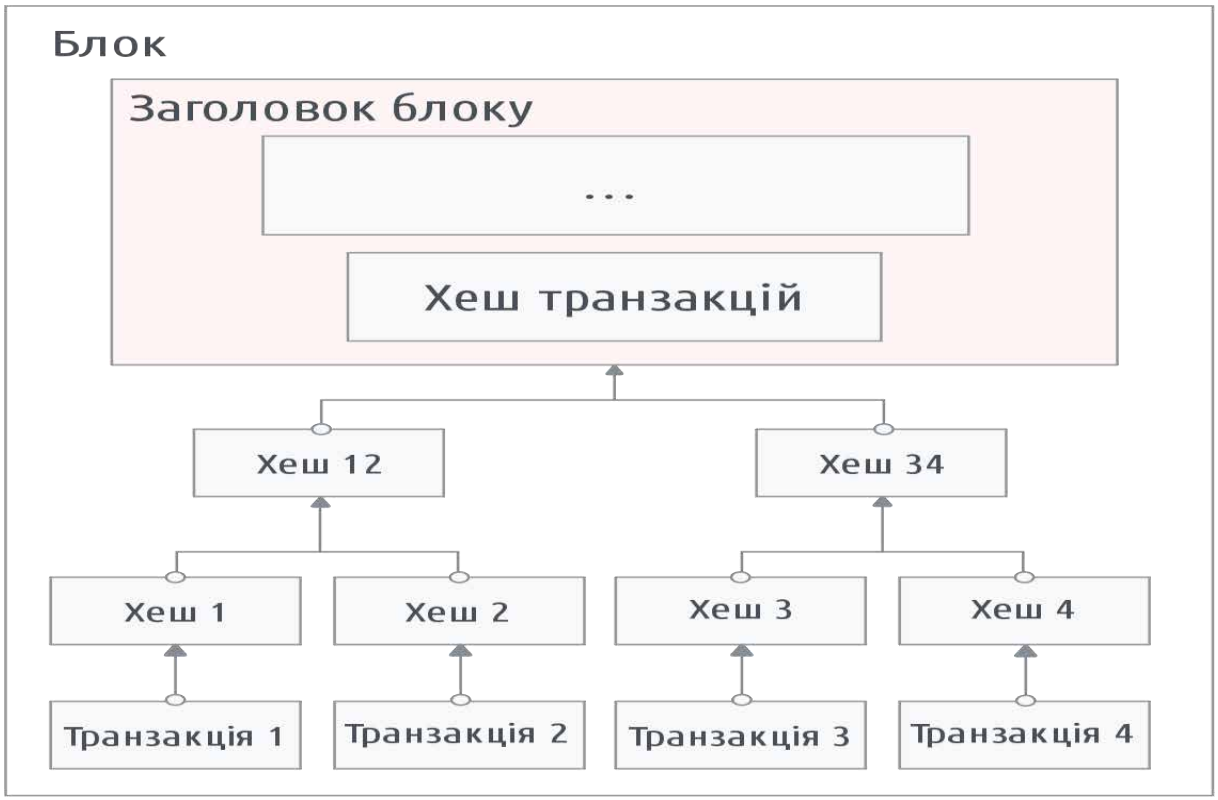

Рисунок 2 – принцип роботи блокчейну [11].

Не менш важливим у розгляді біткоїну є питання майнінгу. Термін майнінг буквально означає видобуток корисних копалин, однак у цифровому світі його сенс полягає у процесі додавання інформаційного блоку, з якого виробляється випуск нових біткоїнів в обіг. Грубо кажучи, будь-яка людина з доступом в інтернет може зайнятися здобиччю біткоїнів. Зараз вже навіть діють варіанти хмарного майнінгу, підключитися до якого можна за допомогою укладання та оплати контракту певний період. Якщо на початку запуску біткоїну учасник міг генерувати монети за допомогою одного комп'ютера, то з розвитком такої системи потужності стало критично не вистачати. Почали з'являтися цілі майнінгові ферми, а згодом і майнінг-пули. Причиною їх створення стало зростання конкуренції та скорочення доступності монет. Ця обставина змусила майнерів об'єднуватись з метою видобування блоку, який вони не могли отримати самостійно. Чим складніше обчислення криптографічних завдань, тим більше ресурсів потрібно їх виконання, насамперед, енергії. Кожен зайнятий у майнінгу мережевий вузол

або комп'ютер збирає інформацію про транзакцію та включає в зашифровану буквенно-цифрову послідовність знаків, звану хешем[20].

Подібно до того, як архівуються документи, процес хешування дозволяє згорнути великі масиви інформації, перетворюючи їх у набагато менший обсяг даних. Залежно від того, який алгоритм хешування задіяний, його результатом буде хеш фіксованої довжини. В криптовалюті використовується алгоритм SHA- 256, який забезпечує отримання хеша завдовжки 64 знаки. Програмне забезпечення на комп'ютері майнера об'єднує хеш першої транзакції разом з усією інформацією з необробленою інформацією наступної не хешованої транзакції, що міститься в ньому, створюючи новий хеш.

Ця процедура повторюється щоразу з надходження у обробку нових транзакцій. Саме таким чином транзакції об'єднуються у будівельні блоки для блокчейну. Особливістю майнінгу криптовалюти є те, що кількість випуску монет обмежена. За задумом С. Накамото, алгоритм видобутку біткоїну влаштований так, щоб генерувати однакова кількість монет за одиницю часу. У перші чотири роки протокол передбачав випуск фіксованої кількості блоків, що містять 50 біткоїнів, до 2012 року число монет скоротилося до 25 і далі ще в 2 рази кожні чотири роки. Теоретично, до 2140 року видобуток повинен припинитися, а загальна кількість монет у обігу складе 21 мільйон. Такий пристрій системи надає біткоїну рідкість, що дозволяє тримати його курс, а також виключає ймовірність інфляції[9].

Головна роль створення криптоактивів полягає в тому, що усуваючи потребу у посереднику, вона підтримує інфраструктуру, у якій незнайомі люди можуть вести бізнес друг з одним. Це досягається за рахунок передачі найважливішої функції ведення облікових регістрів від централізованих фінансових установ до мережі автономних комп'ютерів, що формують розподілену систему довіри, не підконтрольну жодній окремо взятій установі.

У своїй основі криптовалюти будуються на ідеї безлопатевого та універсального облікового регістру, відкритого для громадського користування та постійно контрольованого високопродуктивними

комп'ютерами, які функціонують незалежно один від одного. За рахунок виключення посередників разом з їх комісійними, криптовалюта дозволяє скоротити витрати на ведення бізнесу, а також запобігає корупції, що існувала в посередницьких структурах. Відкритий обліковий регістр, який використовується криптовалютами, виводить на поверхню внутрішній механізм функціонування економіко-політичної системи. Потенціал цієї технології як засобу забезпечення прозорості та контролю простягається набагато далі за фінансові сфери, адже вона здатна усунути будь-яких інформаційних посередників. За своєю сутністю ця технологія є формою соціальної організації, здатну передати контроль грошових потоків та інформації від могутньої еліти простим людям. Це дозволить повернути їм право вільно розпоряджатися своїми активами та талантами[18].

Таким чином, можна зробити висновок, що система блокчейна є центром криптовалют, на якому заснована вся їхня робота.

1.2. Проблеми та перспективу розвитку ринку криптовалютюних активів

За Глобальним індексом впровадження криптовалют за 2022 рік Україна посіла 3 місце (табл. 1).

Таблиця 1

ТОП-10 країн за Глобальним індексом впровадження криптовалют (Global Crypto Adoption Index) за 2022 рік

Країна	Загальний рейтинг	Централізована вартість сервісу	Роздрібна централізована вартість послуги	Рейтинг обсягів біржової торгівлі P2P	Значення DeFi	Роздрібна вартість DeFi
В'єтнам	1	5	5	2	7	6
Філіппіни	2	4	4	66	13	5
Україна	3	6	6	39	10	14
Індія	4	1	1	82	1	1
США	5	3	3	111	3	2
Пакистан	6	10	10	50	22	16
Бразилія	7	7	7	113	8	7
Таїланд	8	12	12	61	5	3
Росія	9	8	8	109	11	12

Китай	10	2	2	144	6	4

Загалом, ринки, що розвиваються, домінують у Global Crypto Adoption Index. Світовий банк поділяє країни на одну з чотирьох категорій на основі рівня доходу та загального економічного розвитку, а саме, країни, які мають високий дохід, дохід вище середнього, дохід нижче середнього та низький дохід. Використовуючи цю структуру, виявлено, що дві середні категорії домінують у верхній частині індексу. З ТОП-20 країн у рейтингу:

– десять країн із доходом нижче середнього: В'єтнам, Філіппіни, Україна, Індія, Пакистан, Нігерія, Марокко, Непал, Кенія та Індонезія;

– вісім із доходом вище середнього: Бразилія, Таїланд, Росія, Китай, Туреччина, Аргентина, Колумбія та Еквадор;

– дві країни з високим доходом: США та Великобританія.

На рис. 1 наведено динаміку курсу біткоїна (BTC) / долар США (USD) на підставі щоденних даних за період 01.01.2015 – 31.03.2023 року.

Прогнозування курсу методом експоненційного згладжування, оскільки саме цей метод показав найменшу середню абсолютну помилку (Mean absolute error) на період 01.04.2023 – 21.04.2023 року, наведено на рис. 2.

Прогноз курсу експертів МОФТ на основі даних світових аналітичних платформ, а також авторських оцінок наведено на рис. 3.

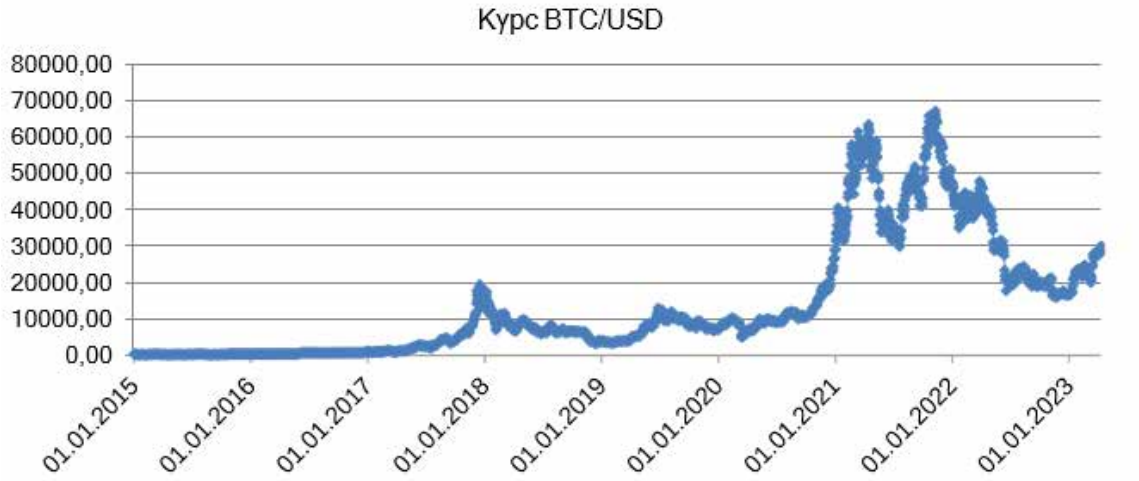

Рис. 1. Динаміка курсу біткоїна (BTC) / долар США (USD)

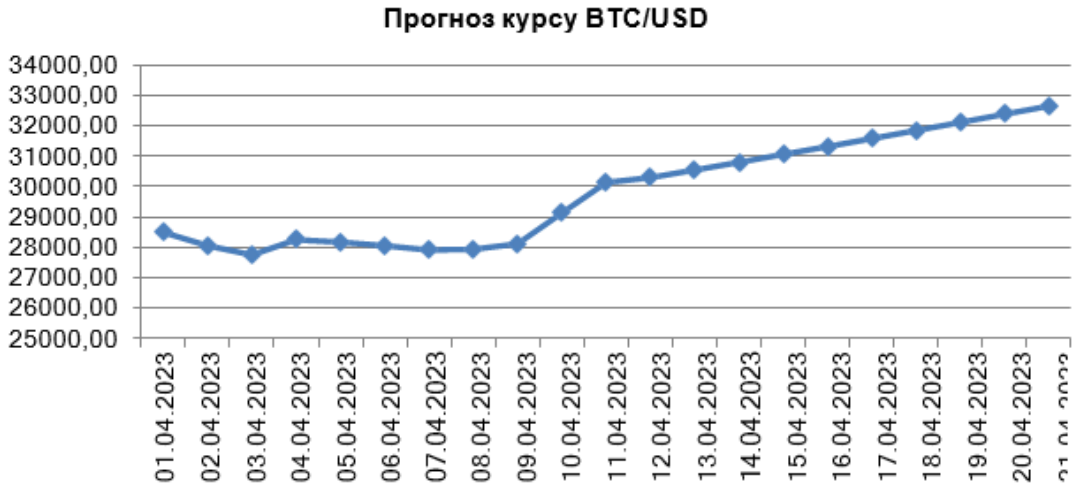

Рис. 2. Прозноз курсу біткоїна (BTC) / долар США (USD)

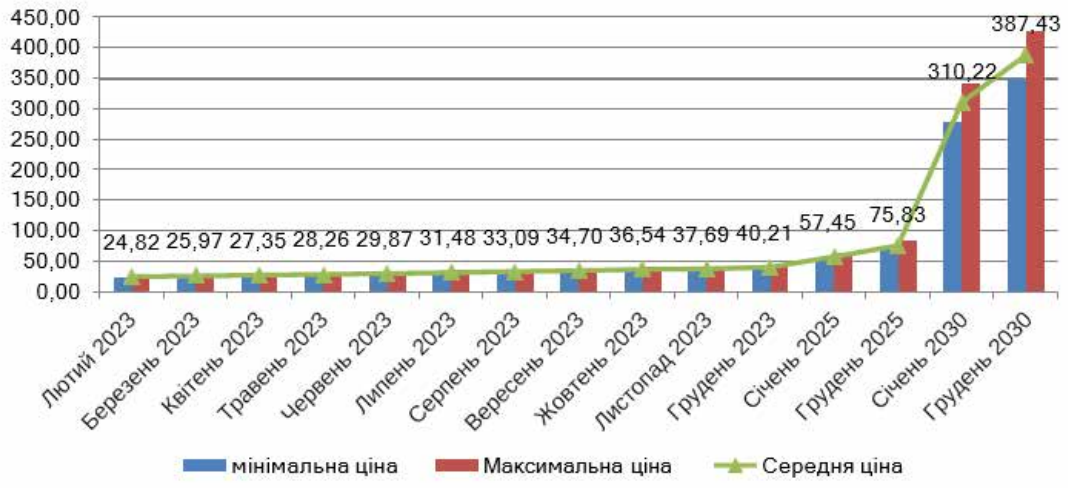

Рис. 3. Прогноз курсу біткоїна на 2023, 2025 та 2030 роки (тис дол. США)

Серед наявних в світі 20000 криптовалют найбільш популярними і вартісними станом на березень 2023 року є Bitcoin, Ethereum, Tether, USD Coin, BNB, XRP, Binance USD, Dogecoin, Cardano та Polygon. Пропонуємо визначити фактори, які найбільше впливають на курс біткоїна за допомогою кореляційного аналізу взаємозалежності:

– курсу криптовалюти біткоїна (BTC) та пар найбільш впливових світових валют, а саме євро / долар США (EUR/USD); китайський юань / долар США (CNY/USD); японська єна / долар США (JPY/ USD); британський фунт / долар США (GBR/USD); австралійський долар / долар США (AUD/USD); швейцарський франк / долар США (CHF/USD);

– курсу біткоїна та світових цін на дорогоцінні метали золото (Au), срібло (Ag), платину (Pt);

– курсу біткоїна та цін цінних паперів на най- більших фондових біржах (індекс PFTS, індекс UX, індекс Dow Jones, індекс S&P 500, індекс NASDAQ, індекс Nikkei, індекс FTSE, індекс Euro STOXX, індекс DAX, індекс SSE).

Модель кореляційної залежності курсу біткоїна та пар найбільш впливових світових валют наведена на рис. 4.

Аналіз отриманих коефіцієнтів кореляції показує, що найбільше курс біткоїна (BTC) взаємопов'язаний з курсом CNY/USD (коефіцієнт кореляції +0,9); JPY/USD (коефіцієнт кореляції +0,87); GBR/USD (коефіцієнт кореляції +0,86). При цьому коефіцієнти кореляції мають позитивне значення, що передбачає, що зі збільшенням курсів зазначених валют зростає й курс біткоїна. При цьому курси CHF/USD та EUR/USD мають слабкий зв'язок із ціною біткоїна.

З огляду на те, що найбільшу кореляційну залежність мають курс біткоїна та китайського юаня до долара США, побудовано регресійну модель даної залежності, яка матиме вигляд:

BTC = -180249 + 1407194 x CNY/USD. (1)

Correlations (Spreadsheet2) Marked correlations are significant at p < , 05000 N = 12(Casewise deletion of missing data)							
	EUR/USD	**CNY/USD**	**JPY/USD**	**GBP/USD**	**AUD/USD**	**CHF/USD**	**BTC/USD**
EUR/USD	1,00	0,65	0,74	0,74	0,48	0,66	0,55
CNY/USD	0,65	1,00	0,94	0,92	0,91	0,81	0,90
JPY/USD	0,74	0,94	1,00	0,98	0,87	0,91	0,87
GBP/USD	0,74	0,92	0,98	1,00	0,90	0,90	0,86
AUD/USD	0,48	0,91	0,87	0,90	1,00	0,81	0,84
CHF/USD	0,66	0,81	0,91	0,90	0,81	1,00	0,67
BTC/USD	0,55	0,90	0,87	0,86	0,84	0,67	1,00

Рис. 4. Модель кореляційної залежності курсу біткоїна та пар найбільш впливових світових валют

Побудована модель є адекватною за критеріями Фішера, Стьюдента, Дарбіна-Уотсона.

Отримані результати кореляційного аналізу залежності вартості біткоїна від вартості золота, срібла та платини на торгах LBM (London Gold Fixing) наведено на рис. 5.

Correlations (Spreadsheet2) Marked correlations are significant at p < ,05000 N = 12(Casewise deletion of missing data)				
	Au	**Ag**	**Pt**	**BTC**
Au	1,00	0,87	0,48	0,80
Ag	0,87	1,00	0,80	0,62
Pt	0,48	0,80	1,00	0,25
BTC/USD	0,80	0,62	0,25	1,00

Рис. 5. Модель кореляційної залежності курсу біткоіна (BTC) та вартості дорогоцінних металів

Результати показують, що найбільшим чином курс біткоїна взаємопов'язаний з курсом золота (коефіцієнт кореляції +0,87).

З огляду на те, що найбільшу кореляційну залежність мають курс біткоїна та вартість золота, побудовано регресійну модель даної залежності, яка матиме вигляд:

BTC = -138945 + 94 x Au. (2)

Отримані результати кореляційного аналізу залежності вартості біткоїна від вартості цінних паперів на найбільших фондових біржах наведено на рис. 6.

Correlations (Spreadsheet2) Marked correlations are significant at p < , 05000 N = 12 (Casewise deletion of missing data)											
	PFTS	**UX**	**Dow Jones**	**S&P 500**	**NASDAQ**	**Nikkei**	**FTSE**	**Euro STOXX**	**DAX**	**SSE**	**BTC/USD**
PFTS	1,00	0,31	0,69	0,73	0,74	0,46	0,38	0,79	0,79	0,61	0,43
UX	0,31	1,00	0,30	0,56	0,63	-0,08	0,45	0,30	0,40	0,62	0,69
Dow Jones	0,69	0,30	1,00	0,92	0,83	0,69	0,81	0,97	0,96	0,56	0,65
S&P 500	0,73	0,56	0,92	1,00	0,98	0,58	0,76	0,90	0,90	0,70	0,93
NASDAQ	0,74	0,63	0,83	0,98	1,00	0,50	0,65	0,83	0,83	0,74	0,96
Nikkei	0,46	-0,08	0,69	0,58	0,50	1,00	0,50	0,67	0,62	0,26	0,16
FTSE	0,38	0,45	0,81	0,76	0,65	0,50	1,00	0,81	0,84	0,31	0,59
Euro STOXX	0,79	0,30	0,97	0,90	0,83	0,67	0,81	1,00	0,99	0,57	0,60
DAX	0,79	0,40	0,96	0,90	0,83	0,62	0,84	0,99	1,00	0,58	0,64
SSE	0,61	0,62	0,56	0,70	0,74	0,26	0,31	0,57	0,58	1,00	0,54
BTC/USD	0,43	0,69	0,65	0,93	0,96	0,16	0,59	0,60	0,64	0,54	1,00

Рис. 6. Модель кореляційної залежності курсу біткоїна та вартості цінних паперів на найбільших фондових біржах

Результати показують, що найбільшим чином курс біткоїна взаємопов'язаний з індексом NASDAQ (коефіцієнт кореляції +0,96) та індексом S&P 500 (коефіцієнт кореляції +0,93).

З огляду на те, що найбільшу кореляційну залежність мають курс біткоїна та індекс NASDAQ, побудовано регресійну модель даної залежності, яка матиме вигляд:

BTC = -48421.9 + 6,2 x NASDAQ. (3)

Сучасні глобальні виклики на кшталт кібератакам та шахрайству й крадіжки даних, мають загрозливий характер й щодо розвитку крипто-індустрії для економічного потенціалу держави, що провокує нові завдання перед спецслужбами. Шахраї створюють власні фіктивні проекти фінансових сервісів на блокчейні. Наприклад, спецслужби окремих зарубіжних країн намагаються відслідковувати криповалютні платежі за допомогою нейромереж та виявляють кіберзлочинців, які мають ключі для відкриття біткоїн-гаманців [10]. Основні виклики функціонування індустрії крипто-валют представлено на рис. 7.

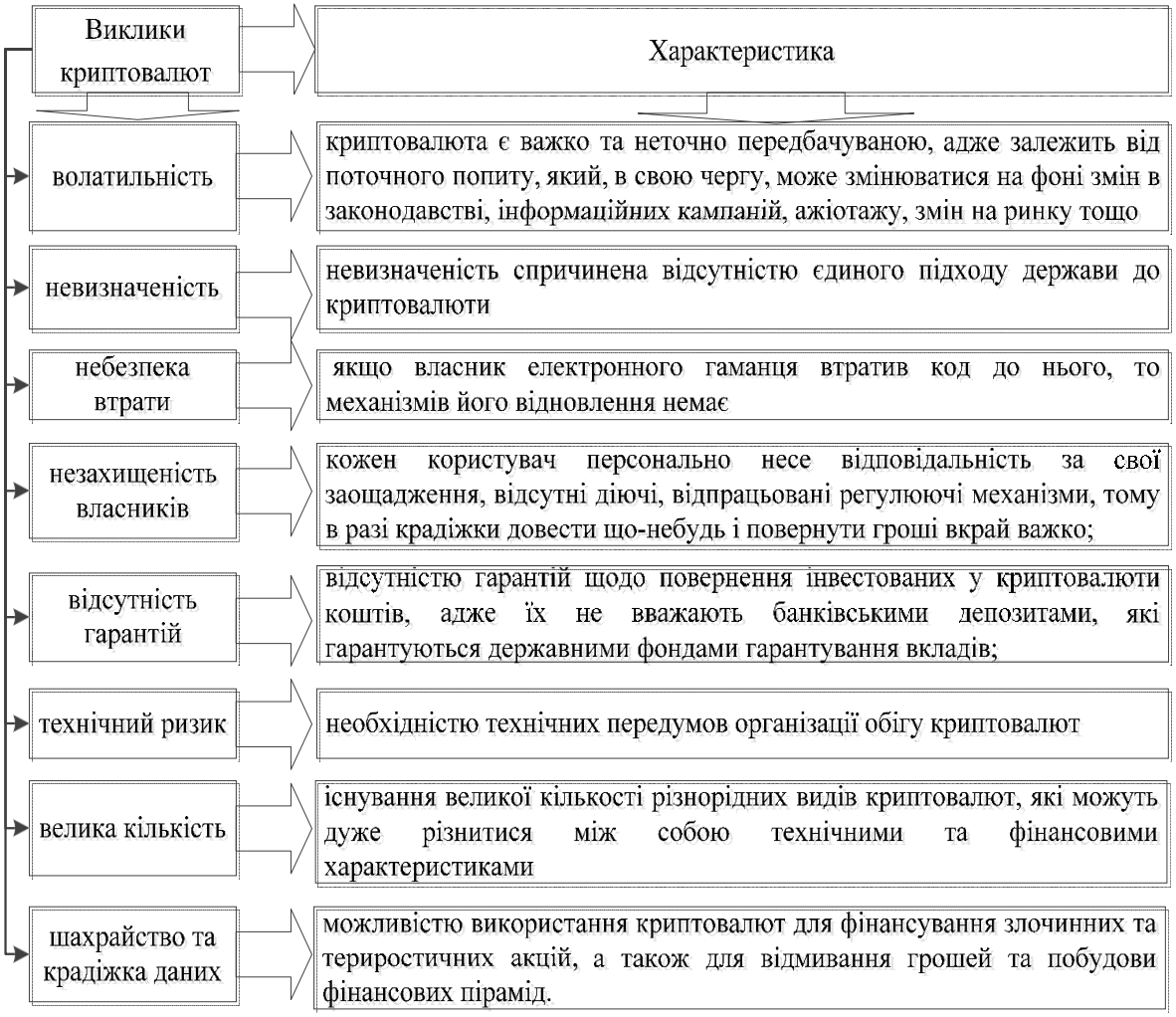

Рис. 7. Основні виклики функціонування індустрії криптовалют

1.3. Концептуальні засади моделювання стратегії захисту криптовалютних активів

У сучасному цифровому світі, де криптовалюти здобувають все більше популярності, захист криптовалютних активів стає надзвичайно важливою проблемою. Збільшення кількості кібератак та зловмисних дій призводить до необхідності розробки ефективних стратегій захисту.

Захист криптовалютних активів став важливою складовою в сучасній кібербезпеці. Зростання кількості кіберзлочинів і кібератак, спрямованих на віртуальні гаманці та торговельні платформи, свідчить про актуальність проблеми. Відсутність централізованого контролю та відкритість криптовалют роблять їх привабливим об'єктом для кіберзлочинців.

Однією з ключових концептуальних засад є забезпечення комплексної фізичної та кібербезпеки. Це включає в себе не лише використання захисних програм та антивірусів, а й встановлення надійних механізмів фізичного контролю доступу до засобів зберігання ключів. Врахування інтеграції фізичних та віртуальних заходів безпеки є важливим аспектом стратегії.

Фізична безпека в контексті криптовалют передбачає реалізацію заходів для фізичного захисту пристроїв та засобів зберігання криптовалютних ключів. Це включає в себе використання безпечних фізичних приміщень, де знаходяться сервери та обладнання, а також встановлення механізмів контролю доступу, які обмежують фізичний доступ до цих приміщень.

Кібербезпека орієнтована на захист від кіберзагроз та атак у віртуальному просторі. Це включає в себе використання сучасних технологій та програмного забезпечення, таких як антивіруси та фаєрволи, для виявлення та запобігання зловмисних програм і кібератак.

Однак, ефективна захист фінансових активів потребує інтеграції фізичних та кіберзаходів. Наприклад, фізичний контроль доступу до

серверних кімнат повинен супроводжуватися електронним контролем, який реєструє та моніторить активність користувачів. Такий комплексний підхід дозволяє ефективно виявляти та запобігати несанкціонованому доступу та можливим загрозам.

Суспільство стикається зі стрімким розвитком криптовалют та блокчейн-технологій, що ставить питання безпеки зберігання та обробки криптовалютних активів у цифровому середовищі. Наступ на ці активи може мати серйозні наслідки, тому розробка ефективної стратегії захисту є вельми актуальною проблемою.

Моделювання стратегії захисту криптовалютних активів є складним завданням, що вимагає комплексного підходу та врахування різноманітних аспектів безпеки. Послідовна інтеграція концептуальних засад, таких як фізична та кібербезпека, контроль доступу, шифрування даних, аудит та моніторинг, освіта та навчання, апаратний захист та юридична безпека, сприяє створенню ефективної стратегії, що гарантує безпеку та стійкість криптовалютних активів у цифровому вимірі. Фізична безпека та кібербезпека є взаємопов'язаними аспектами, об'єднуючи фізичні та віртуальні шари безпеки, щоб максимально захистити криптовалютні активи від потенційних ризиків.

Контроль доступу в контексті захисту криптовалютних активів включає в себе комплексний підхід для регулювання прав і можливостей користувачів у системі. Ця концепція передбачає управління тим, хто і як має доступ до цифрових ресурсів, включаючи криптовалютні гаманці та дані транзакцій.

Основною метою контролю доступу є забезпечення конфіденційності та цілісності інформації. Це означає, що лише авторизовані особи мають право переглядати, редагувати або виконувати операції з криптовалютними активами.

Використання складних паролів, які важко вгадати, та впровадження механізмів двофакторної аутентифікації є елементами контролю доступу для

підвищення безпеки. Додатково, розподіл прав доступу відповідно до ролей та функцій користувачів зменшує ризик можливого зловживання привілеїв.

Контроль доступу також передбачає аудит та моніторинг. Аудит дозволяє реєструвати всі дії користувачів, а моніторинг дозволяє в реальному часі виявляти аномальні або підозрілі активності. Це не тільки допомагає у виявленні можливих загроз, але й створює базу для подальшого аналізу та вдосконалення стратегії захисту.

Загальний принцип контролю доступу полягає в тому, щоб забезпечити правильний баланс між безпекою та зручністю використання для легітимних користувачів, забезпечуючи при цьому ефективний захист криптовалютних активів від недозволеного доступу та зловживання.

Шифрування даних – це техніка захисту інформації, що передбачає перетворення звичайного тексту (даних) у незрозумілий код (шифр) за допомогою спеціального алгоритму та ключа. Основна мета полягає в тому, щоб у випадку несанкціонованого доступу або перехоплення інформації, зловмисники не мали можливості зрозуміти чи використовувати отримані дані без відповідного ключа.

В контексті криптовалют, шифрування є критично важливим елементом безпеки, оскільки розкриття ключової інформації, такої як приватні ключі, може призвести до непередбачуваних наслідків. Використання сучасних криптографічних алгоритмів дозволяє ефективно захищати конфіденційність та цілісність фінансових даних.

Шифрування може бути симетричним або асиметричним. У симетричному шифруванні використовується один ключ для як шифрування, так і розшифрування інформації. У випадку асиметричного шифрування використовуються пари ключів: публічний та приватний. Публічний ключ використовується для шифрування, а приватний — для розшифрування.

Важливим аспектом є безпека самого ключа. Збереження ключів в безпечному місці та регулярна їх зміна є обов'язковими практиками. Також важливо враховувати сучасні тренди та розвиток кіберзагроз, оскільки

алгоритми, які сьогодні є безпечними, можуть стати застарілими в майбутньому. Тому, постійне оновлення методів шифрування — це необхідна умова для забезпечення стійкої захищеності фінансових активів.

Аудит та моніторинг є невід'ємними компонентами стратегії захисту криптовалютних активів, спрямованими на виявлення та реагування на потенційні безпекові загрози.

Аудит означає систематичне оглядання та оцінювання процесів, систем та дій з метою визначення відповідності певним стандартам чи визначеним правилам. У контексті криптовалют, аудит включає в себе регулярну перевірку систем безпеки, виявлення слабких місць, аналіз журналів подій та інших аспектів, що стосуються безпеки інформації.

Моніторинг — це постійна спостережливість за системами та мережами з метою виявлення аномальної чи підозрілої активності. Моніторинг в реальному часі дозволяє оперативно реагувати на події, що можуть свідчити про можливий інцидент безпеки. Наприклад, система моніторингу може виявити невідомі або невипадкові підключення до системи або надто активну діяльність, яка вказує на атаку чи вторгнення.

Важливим аспектом є аналіз журналів подій, який надає інформацію про всі дії, які відбуваються в системі. Ретельний аудит журналів може виявити аномальні патерни, несподівані запити чи інші підозрілі активності.

Об'єднання аудиту та моніторингу дозволяє не лише реагувати на події в реальному часі, але і забезпечити систему навчання для вдосконалення стратегії захисту в майбутньому. Спостереження за активністю та аналіз інцидентів дозволяють покращити безпекові заходи та призначити заходи для подальшого зміцнення захисту.

Освіта та навчання грають критичну роль у створенні свідомих та кібербезпечних користувачів криптовалют. Це охоплює різні аспекти, спрямовані на розуміння ризиків та відповідального використання цифрових фінансових інструментів.

Освіта має на меті навчити користувачів розпізнавати соціально-інженерні атаки, які можуть включати в себе шахрайство, фішингові атаки, чи інші форми маніпуляції з метою отримання конфіденційної інформації.

Навчання повинно охоплювати використання безпечних практик, таких як встановлення складних паролів, двофакторна аутентифікація, та правила безпечного зберігання і обробки криптовалют.

Користувачі повинні розуміти правові аспекти використання криптовалют та обов'язки в рамках регуляторних вимог. Це може включати в себе податкові аспекти, обов'язки відповідно до законодавства про фінансовий моніторинг та інші аспекти правової безпеки.

Користувачі повинні бути навчені взаємодії з різними видами гаманців, включаючи вибір надійних апаратних гаманців та правила безпечного зберігання приватних ключів.

У світі швидко мінливих технологій, освіта повинна бути постійно оновлюваною. Користувачам слід отримувати актуальну інформацію про нові загрози та стратегії захисту.

Користувачі повинні бути навчені ефективному реагуванню на можливі інциденти, включаючи швидке повідомлення про підозрілу активність та співпрацю зі службами підтримки чи правоохоронними органами.

Розуміння цих аспектів не тільки забезпечить індивідуальну безпеку користувачів, але й сприятиме загальній стійкості та безпеці криптовалютного середовища.

Апаратний захист у контексті криптовалют відіграє важливу роль у збереженні приватних ключів та іншої конфіденційної інформації. Апаратні гаманці є одним із прикладів, де приватні ключі зберігаються в офлайн середовищі, у вигляді фізичного пристрою. Це робить їх менш вразливими до кібератак, оскільки для здійснення зловмисної дії потрібно фізичний доступ до самого пристрою.

При використанні апаратних рішень, таких як апаратні гаманці, важливо враховувати їхню надійність і виробника, адже вони виступають як фізичні

тримачі криптовалютних активів. Забезпечення надійного апаратного захисту передбачає ретельний відбір та використання відомих та перевірених виробників.

Юридична безпека включає в себе дотримання регуляторних вимог та створення умов для захисту прав та інтересів користувачів у юридичних рамках. Регулятивне середовище для криптовалют постійно змінюється, і, отже, важливо розуміти та дотримуватися відповідних законів та нормативів.

Це включає в себе:

1. Регуляторні обмеження:

Розуміння та дотримання обмежень, які регулюють використання криптовалют у різних юрисдикціях.

2. Податкова політика:

Знання податкових обов'язків, пов'язаних із володінням, обміном та торгівлею криптовалютами.

3. Конфіденційність і право на захист даних:

Врахування нормативів, що стосуються захисту особистих даних користувачів у контексті криптовалютних операцій.

4. Легальні взаємини з фінансовими установами:

Розуміння та дотримання вимог для легальної взаємодії з банками та іншими фінансовими установами.

5. Захист від шахрайства та правозахист:

Виявлення і дії у випадку можливого шахрайства та забезпечення правозахисту користувачів у випадках спорів чи інцидентів.

Юридична безпека важлива для збереження довіри до криптовалют, адже вона створює умови для легального та безпечного використання цифрових активів.

Першим кроком у розробці стратегії захисту є аналіз потенційних загроз. Це включає в себе вивчення методів атак, які використовуються зловмисниками для витягування конфіденційної інформації або здійснення

крадіжок. Особлива увага приділяється аналізу соціально-інженерних аспектів, фішингових атак та атак на основі витоків даних.

Однією з ключових концепцій є визначення компонентів стратегії захисту. Це включає в себе розробку механізмів двофакторної аутентифікації, шифрування даних, контроль доступу та моніторинг транзакцій. Забезпечення безпеки на рівні технічних, організаційних та правових аспектів є важливою складовою стратегії.

Моделювання стратегії захисту передбачає розробку ефективної моделі виявлення загроз. Використання сучасних алгоритмів машинного навчання та штучного інтелекту дозволяє вчасно виявляти підозрілу активність та запобігати можливим атакам.

Однією з важливих складових стратегії захисту є навчання користувачів. Свідомість про загрози та вміння виявляти підозрілу активність допомагає у підвищенні рівня безпеки. Крім того, важливо розглядати соціальну відповідальність у розробці та використанні криптовалютних технологій.

Моделювання стратегії захисту криптовалютних активів є складним завданням, яке вимагає комплексного підходу. Аналіз потенційних загроз, визначення ключових компонентів стратегії, розробка моделі виявлення загроз та соціальна відповідальність є важливими кроками у забезпеченні безпеки криптовалютних активів у сучасному цифровому середовищі.

Висновки до 1 розділу

У першому розділі магістерської роботи було проведено аналіз технології блокчейн як основи функціонування криптовалют. Розглянуті ключові аспекти її структури та принципи роботи, що утворюють невід'ємну основу для розуміння проблем та викликів, які виникають при управлінні криптовалютними активами.

Далі, зосередившись на ринку криптовалютних активів, були ідентифіковані поточні проблеми та розглянуті перспективи їх розвитку.

Зокрема, була звернута увага на волатильність цін, регуляторні питання, а також потребу у більшій стабільності та визначеності для підтримки інвесторського інтересу.

Особливий акцент у розділі був зроблений на концептуальних засадах моделювання стратегії захисту криптовалютних активів. Досліджені аспекти фізичної безпеки та кібербезпеки, контролю доступу, шифрування даних, аудиту та моніторингу, освіти та навчання, апаратного захисту та юридичної безпеки. Цей аналіз визначив ключові компоненти ефективної стратегії захисту, які взаємодіють для забезпечення інтегрованого підходу до безпеки криптовалютних активів.

Отже, результати аналізу та обговорення теоретичних засад створюють основу для подальшого дослідження та розробки практичних заходів з захисту криптовалютних активів, що є об'єктом подальших розділів магістерської роботи.

РОЗДІЛ 2
МОДЕЛЮВАННЯ ПРОЦЕСІВ ЗАХИСТУ КРИПТОВАЛЮТНИХ АКТИВІВ ТА ЇХ НАСЛІДКИ

2.1. Технологічні аспекти захисту криптовалютних активів

У світі електронних фінансів інновації часто супроводжуються новими викликами, а це особливо стосується криптовалютних активів. Все починалося з введення Bitcoin в 2009 році, і з того часу криптовалюти стали не лише об'єктом інвестицій, але і об'єктом величезної уваги злочинців і кіберзлочинців.

З кожним пройденим роком криптовалюти набувають все більшого значення в світі фінансів, стаючи важливим інструментом для глобальних транзакцій та інвестування. Проте разом із зростанням популярності криптовалют, збільшується ймовірність кібератак, зловживань та інших загроз для їхньої безпеки.

Криптовалюти, виступаючи новаторськими фінансовими інструментами, привертають увагу як інвесторів, так і зловмисників. Розгляд та аналіз основних загроз, які ставлять під загрозу безпеку криптовалютних активів, є критичним етапом для розробки та вдосконалення заходів захисту. Основні аспекти цих загроз включають кібератаки, соціальний інжиніринг та використання шкідливих програм.

Кібератаки на криптовалютні активи представляють серйозну загрозу для стабільності та безпеки цього нового класу активів. Розглядаючи аспекти кібератак, необхідно звернутися до різних форм атак, які мають вплив на різні елементи криптовалютної інфраструктури.

Атаки на блокчейн мережі можуть мати серйозні наслідки для її цілісності та довіри користувачів. Атака 51% - це форма атаки, коли одна сторона здобуває контроль над більшістю обчислювальної потужності мережі, що дає їй можливість змінювати та відхиляти транзакції. Для захисту від таких

атак, розробники блокчейнів використовують вдосконалені алгоритми консенсусу, такі як Proof-of-Stake (PoS) або Delegated Proof-of-Stake (DPoS), які ускладнюють спроби зловмисників маніпулювати мережею.

Майнінгові пули, де група майнерів об'єднує свої ресурси для спільного видобутку блоків, також стають об'єктом кібератак. Атаки можуть бути спрямовані на видалення чи модифікацію транзакцій, спрямованих до мережі. Захист включає в себе використання захищених протоколів комунікації та постійний моніторинг активності пулів.

Криптобіржі є центральними точками обміну та торгівлі криптовалютами, тому вони стають особливо привабливим об'єктом для кібератак. Від вторгнень через вразливості в програмному забезпеченні до атак DDoS, мета атак може бути різноманітною – від викрадення коштів до розкриття особистої інформації користувачів. Захист криптобірж включає в себе регулярні аудити безпеки, шифрування даних, а також розвинені системи виявлення та відповіді на інциденти.

Атаки DDoS на криптовалютні платформи можуть викликати перебої у роботі платформи, що призводить до неможливості здійснення торгів та інших операцій. Захист включає в себе використання технологій для виявлення та фільтрації трафіку, а також резервних систем для забезпечення доступності платформи під час атак.

Смарт-контракти, що є основою багатьох криптовалютних платформ, можуть бути об'єктом атак через вразливості в їхньому коді. Зловмисники можуть експлуатувати ці вразливості для виведення коштів або навіть для впровадження зловмисного коду в блокчейн. Використання безпечних розробницьких практик та аудитів коду є критичним для забезпечення захисту смарт-контрактів.

Способи соціального інжинірингу та фішингу, які спрямовані на користувачів криптовалют, можуть включати в себе виведення конфіденційної інформації, аутентифікаційних даних та приватних ключів. Навчання користувачів, щоб вони розпізнавали потенційно шкідливі сценарії та

впровадження двофакторної аутентифікації можуть виявитися ефективними стратегіями для запобігання атакам соціального інжинірингу.

Використання шкідливих програм для викрадання криптовалют стало однією з найпоширеніших загроз. Шкідливі програми можуть включати в себе віруси, троянські коні, різновиди шифрувальних програм та інші види шкідливого програмного забезпечення. Важливою частиною захисту є вдосконалені системи антивірусного захисту, регулярні оновлення програмного забезпечення та постійний моніторинг на наявність невідомих або підозрілих програм.

Загрози, які виникають з кібератак на криптовалютні активи, вимагають постійного вдосконалення технічних засобів захисту. Інноваційні рішення, які включають в себе кіберзахист, аналіз безпеки та технології блокчейн, є необхідними для того, щоб гарантувати безпеку користувачів та довіру глобальної громадськості до криптовалют як перспективного фінансового інструменту.

Гаманці (або криптовалютні гаманці) та приватні ключі є критичними компонентами безпеки криптовалют. Атаки, спрямовані на отримання несанкціонованого доступу до гаманців або витіснення приватних ключів, можуть призвести до втрати коштів. Зловмисники можуть використовувати різні методи, такі як фішинг, соціальний інжиніринг або атаки на програмне забезпечення, щоб отримати доступ до гаманців. Захист включає в себе використання хардверних гаманців, які зберігають ключі в офлайн-середовищі, та використання заходів безпеки для захисту гаманців від несанкціонованого доступу.

Смарт-контракти, розглядаючи їх як програмні коди, також є об'єктом кібератак. Вразливості в коді смарт-контрактів можуть призвести до їхнього експлуатації та втрати коштів. Забезпечення аудиту безпеки смарт-контрактів, використання найсучасніших методів розробки та постійний моніторинг за можливими вразливостями є необхідними для запобігання атак на смарт-контракти.

Атаки на програмне забезпечення можуть спрямовуватися на отримання приватних ключів користувачів. Використання шкідливих програм, які відслідковують введення користувача або намагаються знайти та витягнути приватні ключі, може призвести до втрати доступу до гаманців та криптовалютних активів. Заходи безпеки включають в себе захист від шкідливих програм, регулярне оновлення антивірусного та антишпигунського програмного забезпечення та використання хардверних рішень для зберігання приватних ключів.

Сучасні загрози для криптовалютних активів вимагають постійного удосконалення методів захисту, використання новітніх технологій та посилення кіберзахисту на всіх рівнях інфраструктури. Спільні зусилля галузі, регуляторів та розробників технологій є критичними для того, щоб забезпечити безпеку та довіру у цьому динамічному сегменті фінансового світу.

Кібератаки на криптовалютні активи представляють значущу загрозу для їхньої стабільності, цілісності та довіри. Аспекти кібератак, включаючи атаки на блокчейн мережі, майнінгові пули, криптобіржі, смарт-контракти та особисті гаманці, демонструють різноманітність методів, які зловмисники можуть використовувати для отримання неприпустимого доступу та втручання.

Загальна безпека криптовалютних активів вимагає не тільки технічних заходів, але й співпраці галузі, правозахисних органів та регуляторів для розробки ефективного інфраструктурного захисту. Світ криптовалют повинен постійно адаптуватися до еволюції кіберзагроз, змінюючи свої підходи та вдосконалюючи технічні стандарти безпеки.

Соціальний інжиніринг представляє собою використання маніпуляції та обману людей для отримання конфіденційної інформації або здійснення несанкціонованих дій. У сфері криптовалют соціальний інжиніринг став значущою загрозою, оскільки кіберзлочинці використовують психологічні та

соціальні методи, щоб отримати доступ до гаманців, приватних ключів та іншої конфіденційної інформації користувачів.

Фішинг є однією з найпоширеніших форм соціального інжинірингу в криптосфері. Атаки фішингу включають в себе намагання здійснити введення в оману, представляючись довіреними джерелами. Наприклад, кіберзлочинці можуть висилати електронні листи, які імітують офіційні повідомлення від криптобірж, запитуючи від користувачів їхні особисті дані чи приватні ключі. Захист від фішингу вимагає ефективної системи фільтрації спаму, освіти користувачів та ретельного вивчення електронних повідомлень для виявлення неправомірних запитань.

Соціальні мережі стали плодючим ґрунтом для соціального інжинірингу в області криптовалют. Зловмисники можуть використовувати важливі дані з профілів користувачів, щоб створювати персоналізовані атаки. Зазвичай це може включати в себе створення фейкових облікових записів або відправку запитань у приватні повідомлення з пропозиціями, які здаються надто вигідними, щоб відмовитися від них. Спілкування в соціальних мережах може також використовуватися для розповсюдження шкідливих посилань або програмного забезпечення.

Зловмисники можуть намагатися обдурити користувачів, представляючись важливими особистостями в криптоспільноті, які можуть надавати поради чи пропозиції для інвестування. Це може включати в себе імітацію відомих блогерів, інвесторів чи представників криптобірж. Захист від імперсонації включає в себе ретельну перевірку профілів та уникає погодження на сумнівні запитання або пропозиції від невідомих осіб.

Атаки, які використовують соціальний інжиніринг під прикриттям технічної підтримки, можуть включати в себе виклик до користувача від уявленого представника криптобіржі або розробника, який вказує на те, що у них виникли проблеми з обліковим записом та потрібна допомога. В результаті цього користувачам може бути запропоновано розкрити свої аутентифікаційні дані чи навіть приватні ключі. Захист включає в

себе вдосконалення процесів перевірки та аутентифікації для підтвердження ідентичності сторін у комунікації.

Освіта користувачів та підвищення їхньої свідомості про ризики соціального інжинірингу є ключовим елементом захисту. Важливо навчати користувачів розпізнавати підозрілі сценарії та надавати рекомендації щодо безпеки:

- розпізнавання фішингових атак: Користувачі повинні бути навчені виявляти неправдоподібні електронні повідомлення, перевіряти електронні адреси та утримуватися від надання конфіденційної інформації через ненадійні канали.

- безпека в соціальних мережах: Користувачам слід було пояснити, як контролювати налаштування конфіденційності та обмежувати доступ до особистої інформації, а також бути обережними у спілкуванні з незнайомими особами.

- довіра до перевірених джерел: Користувачі повинні розуміти важливість перевірки автентичності сповіщень, особливо тих, які стосуються фінансових операцій або безпеки активів.

- обережність в спілкуванні: Користувачам слід відмовлятися від надання особистої інформації або приватних ключів навіть в тих випадках, коли це вимагається під якимось приводом, до якого вони не мають повної довіри.

- захист від імперсонації: Сприяти збільшенню обізнаності користувачів щодо можливості імперсонації та підкреслення важливості перевірки профілів та взаємодії з відомими та перевіреними особами.

- оновлення знань: Оскільки схеми соціального інжинірингу постійно еволюціонують, важливо, щоб користувачі регулярно оновлювали свої знання та були свідомими останніх трендів у цій області.

Шлях до успішного захисту від соціального інжинірингу включає не лише технічні заходи, але й активну участь та усвідомленість кінцевих користувачів. Регулярна освіта та підвищення рівня кіберсвідомості грають

критичну роль у створенні ефективної системи безпеки в контексті криптовалют та блокчейн технологій.

Використання шкідливих програм є однією з найпоширеніших та серйозних загроз для криптовалютних активів. Шкідливі програми включають в себе віруси, троянські коні, рансомвари, кейлогери, шпигунське програмне забезпечення та інші види зловмисних кодів. Ці програми спрямовані на викрадання конфіденційної інформації, особистих даних або приватних ключів, а також на втручання в операції користувачів з криптовалютами.

Віруси та троянські коні є формами шкідливих програм, які можуть вражати комп'ютери користувачів і використовувати їх для виконання незаконних операцій. Віруси можуть розповсюджуватися шляхом заражених файлів або програм, в той час як троянські коні можуть діяти як приховані програми, здатні виконувати дії без знання користувача. Ці програми можуть бути спрямовані на викрадання особистих даних, включаючи дані для доступу до криптогаманців або облікових записів на криптобіржах.

Рансомвари – це вид шкідливих програм, які блокують доступ користувача до його системи або даних та вимагають викупу за їх розблокування. У контексті криптовалют, рансомвари можуть направлятися на блокування доступу до гаманців або приватних ключів. Це створює ситуацію, коли користувачеві доводиться виплачувати викуп зловмиснику, щоб повернути доступ до своїх цифрових активів.

Кейлогери - це програми, які записують натискання клавіш користувача і використовують цю інформацію для здобуття паролів та інших конфіденційних даних. Шпигунське програмне забезпечення здійснює відстеження активності користувача, включаючи введення миші та натискання клавіш, з метою виявлення конфіденційної інформації.

- Антивірусне програмне забезпечення: Встановлення та регулярне оновлення антивірусних програм може виявити та блокувати шкідливі програми перед їх виконанням.

- Безпека програмного забезпечення: Регулярні оновлення операційних систем та програмного забезпечення можуть усувати вразливості, якими можуть користуватися шкідливі програми.

- Використання хардверних гаманців: Зберігання криптовалютних активів в хардверних гаманцях, які працюють в офлайн-середовищі, може запобігти викраденню приватних ключів.

- Контроль за поштовою скринькою: Обов'язково перевіряйте електронну пошту на наявність спаму і фішингових повідомлень, особливо ті, що стосуються криптовалют.

- Освіта Користувачів: Навчання користувачів розпізнавати потенційно небезпечні ситуації та уникати них.

В умовах постійно зростаючого обсягу шкідливих програм важливо поєднувати технічні заходи безпеки із заходами освіти та превентивної політики для ефективного захисту криптовалютних активів.

Забезпечення безпеки блокчейн мережі є надзвичайно важливим завданням, оскільки ця технологія використовується для зберігання та передачі значущих цифрових активів. Здійснення ефективного захисту вимагає поєднання криптографічних методів, алгоритмів консенсусу, мережевих заходів та систем управління доступом.

Криптографічний Захист

Криптографічний захист є основним стовпом безпеки блокчейн мережі. Включає в себе:

1. Криптографічні хеш-функції

Хеш-функції використовуються для створення унікальних ідентифікаторів (хешів) для блоків та транзакцій. Це дозволяє в реальному часі перевіряти цілісність та автентичність даних в блокчейні.

2. Криптографічні підписи

Цифрові підписи гарантують, що ті, хто взяв участь у транзакції, є власниками своїх приватних ключів. Вони забезпечують відсутність фальсифікації та можливість перевірки автентичності підписів.

3. Шифрування даних

Шифрування даних використовується для захисту конфіденційності даних під час їх передачі та зберігання в блокчейні.

Алгоритми консенсусу

Механізми консенсусу забезпечують узгодженість між всіма учасниками мережі щодо стану блокчейну. Популярні алгоритми консенсусу включають Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS) та інші.

Мережевий Захист

Мережевий захист спрямований на запобігання різноманітним атакам та вразливостям мережі. Включає в себе:

1. Захист від DDOS-атак

Розподілені атаки на відмову в обслуговуванні можуть призвести до відмови блокчейн мережі. Використання систем обмеження швидкості та фільтрації трафіку може запобігти або пом'якшити такі атаки.

2. Вдосконалення протоколів зв'язку

Захист засобів зв'язку між вузлами мережі допомагає уникнути атак перехоплення та модифікації транзакцій.

Управління доступом

Системи управління доступом гарантують, що тільки авторизовані користувачі мають доступ до конкретних функцій мережі та можливість участі в консенсусі.

Моніторинг та виявлення аномалій

Моніторингові інструменти виявляють аномалії в роботі мережі, що може свідчити про атаку. Вони дозволяють оперативно реагувати на потенційні загрози.

Апгрейди та оновлення

Регулярні апгрейди блокчейн мережі допомагають виправляти вразливості та вдосконалювати заходи безпеки на рівні самого протоколу. Апгрейди можуть включати в себе вдосконалення криптографічних

алгоритмів, покращення механізмів консенсусу та впровадження нових заходів безпеки відповідно до мінливих загроз.

Захист від 51% атак

Атака 51% відбувається, коли одна або кілька сторін контролюють більше половини обчислювальної потужності мережі. Це може призвести до зміни історії транзакцій та подвоєння витрат. Захист включає в себе заходи для запобігання або ускладнення таких атак, такі як використання консенсусу Proof-of-Work чи Proof-of-Stake.

Аудит смарт-контрактів

Забезпечення безпеки смарт-контрактів важливо для запобігання вразливостям та використанню їх у зловмисницьких цілях. Регулярні аудити смарт-контрактів допомагають виявити та усунути потенційні проблеми безпеки.

Резервне копіювання та відновлення

Резервне копіювання блокчейн мережі та її даних, включаючи гаманці та ключі, є важливим для гарантування відновлення системи у випадку втрати або пошкодження даних.

Взаємодія з зовнішніми джерелами

Забезпечення безпеки вимагає також обережної взаємодії з зовнішніми джерелами, такими як інші блокчейни, оракули та інші системи. Детальна верифікація та обмеження доступу до таких джерел є важливою для запобігання атак та вразливостей.

Співпраця та обмін інформацією

Блокчейн мережі часто вступають в співпрацю для обміну інформацією про загрози та методи захисту. Взаємодія галузевих гравців дозволяє швидше виявляти та вирішувати проблеми безпеки.

Загальна безпека блокчейн мережі вимагає постійного вдосконалення та адаптації до нових технологічних та кіберзагроз. Інновації у сфері криптографії, мережевих технологій та методів консенсусу грають ключову роль у створенні надійних та стійких до атак блокчейн систем.

Криптографічний захист є вочевидь важливою складовою в галузі кібербезпеки, особливо у контексті технологій блокчейн та криптовалют. Цей підхід забезпечує безпеку та конфіденційність інформації через використання різних криптографічних методів та протоколів.

Криптографічні хеш-функції використовуються для створення унікальних хеш-кодів, що відображають структуру даних, таким чином забезпечуючи цілісність блокчейну. Дані підписуються за допомогою цифрових підписів, що базуються на парах ключів, щоб забезпечити автентичність та відповідальність за транзакції.

Шифрування даних стає важливою складовою для забезпечення конфіденційності інформації, особливо при її трансляції чи зберіганні. У контексті смарт-контрактів, криптографія використовується для забезпечення безпеки виконання контрактів та управління умовами їх реалізації.

Забезпечення стійкості до квантових обчислень стає актуальною задачею у світлі швидкого розвитку цієї технології. Розробка квантостійких криптографічних алгоритмів стає необхідністю для гарантування довгострокової безпеки мережі.

Крім того, криптографія грає ключову роль у захисті від фішингових атак та соціального інжинірингу, забезпечуючи безпечний обмін ключами та важливою узгодженість та взаємодію між різними складовими системи блокчейн.

Регулювання та стандарти в сфері криптовалют та блокчейн технологій є ключовими аспектами, що визначають їхнє функціонування та взаємодію з іншими секторами економіки. У багатьох країнах світу, органи державного управління встановлюють правила та норми для контролю та регулювання цих технологій.

Регулятивна сфера визначає, яким чином криптовалюти, ініціальні монетні пропозиції (ICO), обмінники та інші учасники цього екосистеми повинні функціонувати в межах законів. Деякі країни вже впроваджують законодавство, яке визначає статус криптовалют та встановлює вимоги щодо

їхньої легальності та оподаткування. Також, регуляція визначає, яким чином боротьба з фінансовою злочинністю та запобігання фінансовому тероризму має бути забезпечена в контексті криптовалют.

Стандарти визначають норми та вимоги до різних аспектів розробки, впровадження та експлуатації блокчейн технологій. Це може включати в себе технічні стандарти для реалізації блокчейн протоколів, визначення стандартів безпеки, а також стандарти для сумісності між різними блокчейн платформами. Стандарти є ключовим елементом для забезпечення єднання та взаємодії різних частин цього розмаїття технологічного ландшафту.

Важливим визначником ефективності регулювання є здатність до адаптації до стрімкого темпу інновацій в цій галузі. Зрозуміле та прозоре регулювання, а також розвиток міжнародних стандартів, сприяють стабільності та прийняттю цих технологій як складової частини сучасної економіки.

Захист криптовалютних активів є складним завданням, яке вимагає комплексного підходу та використання передових технологій. Технічні рішення, такі як захист блокчейн мереж, криптографічні методи та ефективні системи регулювання, грають важливу роль у забезпеченні безпеки та стабільності криптовалют.

2.2. Ринкові та соціально-психологічні методи захисту криптовалютних активів

Захист криптовалютних активів є актуальним завданням у зв'язку з постійним розвитком цифрових технологій та зростаючою популярністю криптовалют. Поглиблення розуміння ринкових та соціально-психологічних аспектів є ключовим для розробки ефективних методів захисту цих активів.

Ринкові методи захисту криптовалют:

1. Диверсифікація портфеля: Диверсифікація портфеля є ключовим принципом ризик менеджменту в інвестуванні, включаючи криптовалютні

активи. Цей підхід полягає в розподілі інвестицій між різними видами активів чи ринків з метою зменшення загального ризику та коливань вартості портфеля.

Ідея диверсифікації полягає в тому, щоб не залежати від успіху чи невдачі конкретного активу чи ринку. У контексті криптовалют це означає, що інвестор не повинен концентрувати всі свої кошти в одній криптовалюті, але розподіляти їх між різними криптовалютами чи іншими видами активів.

Основні принципи диверсифікації портфеля:

а) розподіл по видам активів: Інвестор розподіляє свій капітал між різними видами активів, такими як криптовалюти, акції, облігації, нерухомість і т. д. Це дозволяє зменшити вплив негативних змін в одному секторі на загальний портфель.

б) географічна диверсифікація: Розміщення інвестицій в різних географічних регіонах допомагає уникнути ризиків, пов'язаних з економічною чи політичною нестабільністю в конкретних країнах.

в) різноманітність внутрішнього складу: В межах одного виду активу, наприклад, криптовалют, важливо також диверсифікувати портфель. Це означає інвестування в різні криптовалюти з різними характеристиками та потенціалом ринкового зростання.

г) розподіл ризику*: Диверсифікація дозволяє розподілити ризик між різними активами, зменшуючи ймовірність великих втрат в одному напрямку.

Переваги диверсифікації портфеля:

а) зниження загального ризику інвестування.

б) збалансований інвестиційний підхід.

в) захист від значних коливань на ринку.

Можливі виклики та обмеження:

а) не завжди гарантує повне уникнення ризиків.

б) вимагає систематичного моніторингу та перебалансування портфеля.

Враховуючи вищевказані фактори, диверсифікація портфеля залишається важливим інструментом для ефективного управління ризиком при інвестуванні в криптовалютні активи.

2. Технічний аналіз:

Технічний аналіз є важливим інструментом для інвесторів та трейдерів, які працюють з криптовалютами. Цей метод аналізу базується на історичних цінових та обсягових даних для передбачення майбутніх цінових рухів та прийняття обґрунтованих рішень щодо входу чи виходу з позиції.

Основні принципи технічного аналізу:

- графіки та патерни: Технічний аналіз використовує графіки цін для виявлення патернів, таких як голова і плече, подвійне дно чи трендові лінії. Патерни надають інвесторам інформацію про можливі майбутні цінові рухи.

- індикатори та осцилятори: Використання різних технічних індикаторів, таких як RSI (Relative Strength Index), MACD (Moving Average Convergence Divergence), або стохастичний осцилятор, щоб визначити ступінь перекупленості чи перепроданості активу.

- трендовий аналіз: Визначення поточного напрямку ринку і визначення тренду допомагає інвесторам визначити, коли краще увійти або вийти з позиції.

- обсяг торгів: Аналіз обсягів торгів допомагає визначити силу чи слабкість тренду та підтверджує дії на ринку.

Переваги технічного аналізу:

- орієнтований на ціни: Технічний аналіз дозволяє інвесторам аналізувати безпосередньо ціни, що може бути важливим для виявлення патернів та трендів.

- використання історичних даних: Аналізується історична динаміка цін, що дозволяє інвесторам приймати рішення на основі минулих подій.

- використання індикаторів для підтвердження: Використання індикаторів дозволяє інвесторам підтверджувати або спростовувати сигнали ринку.

Можливі виклики та обмеження:

- вплив новин: Технічний аналіз не враховує новини та інші фактори, які можуть впливати на ринок.

- неоглядність на основі історії: Базується на історичних даних, які не завжди відображають майбутні події.

- залежність від розуміння ринку: Вимагає глибокого розуміння технічних показників та їхнього впливу на ринок.

Технічний аналіз є важливим інструментом для трейдерів та інвесторів, які активно взаємодіють з криптовалютами, проте успіх використання цього методу

3. Використання стоп-лос замовлень:

В інвестиційному та трейдерському середовищі використання стоп-лос замовлень вважається важливим елементом стратегії управління ризиком. Цей інструмент дозволяє інвесторам автоматично виходити з позиції, коли ціна активу досягає певного рівня, заздалегідь визначеного інвестором.

Основні аспекти використання стоп-лос замовлень:

а) захист від збитків: Основною метою використання стоп-лос замовлень є мінімізація можливих втрат. Якщо ціна активу падає до певного рівня, замовлення автоматично активується, допомагаючи уникнути подальших збитків.

б) автоматизація рішень: Стоп-лос замовлення забезпечує автоматичний вихід з позиції, що знижує ризик емоційних реакцій та допомагає інвесторові залишатися дисциплінованим у виконанні своїх стратегій.

в) визначення рівня ризику: Інвестор перед відкриттям позиції може визначити точний рівень ціни, на якому він готовий припинити торгівлю. Це дозволяє інвесторові чітко визначити своє ризиковане відношення.

г) динамічне адаптування: Стоп-лос замовлення може бути адаптовано відповідно до ринкової ситуації. Так, інвестор може регулювати рівень стоп-лосу в залежності від змін у ціновій активності.

Переваги використання стоп-лос замовлень:

а) ризиковий контроль: Інвестори можуть активно контролювати рівень ризику, визначаючи точні цінові рівні для виходу з позиції.

б) мінімізація емоційних впливів: Автоматизоване використання стоп-лос замовлень допомагає запобігти емоційному втручанню та необґрунтованим рішенням в гарячих моментах.

в) захист від несприятливих ринкових умов: У разі стрімкого руху цін, стоп-лос замовлення може забезпечити захист від значних втрат.

Можливі виклики та обмеження:

а) потенційні фальшиві вихідні сигнали: В деяких випадках, особливо при волатильних умовах ринку, стоп-лос замовлення може викликати вихід з позиції передчасно через короткочасні коливання цін.

б) залежність від ліквідності: У ринках з обмеженою ліквідністю стоп-лос замовлення може викликати великі проскальзування при виконанні.

в) не гарантує втрати: Існує ризик, що ціна може стрімко змінитися, і стоп-лос не гарантує повного уникнення збитків в умовах ринкової нестабільності.

В цілому використання стоп-лос замовлень є важливим елементом стратегії управління ризиком та дозволяє інвесторам захищати свій капітал в умовах ринкової невизначеності.

Соціально-психологічні методи захисту криптовалютних активів:

1. Едукація інвесторів: Належне розуміння ринкових ризиків та принципів функціонування криптовалют дозволяє інвесторам уникати емоційних реакцій та приймати обґрунтовані рішення.

Едукація інвесторів визнається як важливий елемент успішного та обґрунтованого управління фінансами, зокрема в контексті криптовалютних активів. Цей підхід полягає в наданні інвесторам необхідної інформації, навичок та знань для ефективного прийняття фінансових рішень, а також усвідомлення ризиків та можливостей на ринку криптовалют.

Основні аспекти едукації інвесторів:

а) освіта про криптовалюти: Забезпечення інвесторів базовими знаннями про природу та технологію криптовалют, основні терміни та поняття, роботу блокчейн технологій та основні криптовалютні ринки.

б) розуміння ризиків та потенційних втрат: Навчання інвесторів розпізнавати та оцінювати ризики, пов'язані з криптовалютами, включаючи волатильність ринку, регуляторні аспекти, технічні загрози та інші фактори, які можуть впливати на ціни.

в) технічна грамотність: Надання інвесторам технічних знань, необхідних для використання криптовалютних гаманців, розуміння процесів транзакцій та зберігання цифрових активів.

г) стратегії управління ризиками та портфелем: Навчання інвесторів стратегіям розподілу ризиків, диверсифікації та визначення цілей інвестування.

д) поради щодо безпеки та захисту: Забезпечення інвесторів порадами щодо безпеки, використання двофакторної аутентифікації, вибору надійних гаманців та засобів зберігання, а також уникальних підходів до захисту особистих ключів.

Переваги едукації інвесторів:

- самостійність та самообізнання: Навчання інвесторів створює умови для самостійного прийняття обґрунтованих рішень та розвитку фінансової самообізнаності.

- мінімізація ризиків: Едукація допомагає інвесторам уникнути типових помилок, пов'язаних з невірним розумінням ринку та недостатнім знанням.

- створення інвестиційних спільнот: Розбудова знань та спільноти інвесторів сприяє обміну досвідом та інформацією, що сприяє більш успішному управлінню портфелем.

Можливі виклики та обмеження:

- постійна динаміка ринку: Криптовалютні ринки постійно змінюються, і інвесторам потрібно триматися в тонусі щодо нововведень та тенденцій.

- індивідуальні особливості: Різні інвестори мають різний рівень знань, вмінь та ступінь готовності приймати ризики.

- потреба в систематичному оновленні знань: Швидкий розвиток технологій та ринків вимагає постійного оновлення інвестиційної едукації.

- регуляторні зміни: Зміни в законодавстві та регулюванні криптовалют можуть вплинути на правила та стратегії інвестування.

- психологічний аспект: Едукація також може включати аспекти психології трейдингу, допомагаючи інвесторам розуміти свої емоції та приймати обґрунтовані рішення в умовах стресу та невизначеності.

Роль едукації інвесторів в контексті криптовалют:

а) збільшення легітимності ринку: Інвестори, які розуміють ризики та переваги криптовалют, сприяють створенню легітимного та розвиненого ринку.

б) Створення Інвестиційних Можливостей: За допомогою едукації інвесторів створюється підґрунтя для нових та інноваційних інвестиційних стратегій в сфері криптовалют.

в) зменшення ризику шахрайства: Інвестори, освічені у галузі криптовалют, менше схильні до шахрайства та обману.

г) підвищення свідомості інвесторів: Едукація допомагає створити свідомих та обґрунтованих інвесторів, які розуміють свої цілі та ризики.

д) розвиток індустрії: Інвестори, які розуміють криптовалютні технології та ринок, сприяють загальному розвитку галузі та прискорюють її прийняття в суспільстві.

Едукація інвесторів у сфері криптовалют є ключовим чинником стабільного та ефективного функціонування цього ринку. Цей процес не лише допомагає інвесторам досягти своїх фінансових цілей, але й сприяє створенню стійкої та довіреної екосистеми криптовалют.

2. Медійна грамотність: Інвесторам слід бути свідомими впливу медіа на ринкові тенденції. Розуміння, як інформація впливає на колективну психологію, дозволяє уникати надмірної емоційності в прийнятті рішень.

Медійна грамотність у контексті інвестування в криптовалютні активи визнається як важливий елемент успішного управління портфелем та прийняття обґрунтованих фінансових рішень. Це включає в себе розуміння медійних ресурсів, новин та інформації, які впливають на ринок криптовалют.

Основні аспекти медійної грамотності:

- розпізнавання джерел інформації: Інвестори повинні бути здатні визначати джерела інформації, перевіряти їхню достовірність та розрізняти надійну інформацію від чуток.

- оцінка впливу медіа: Розуміння того, як медіа може впливати на ринок криптовалют та формувати громадську думку, є ключовим для обґрунтованих рішень.

- аналіз інформаційних потоків: Інвесторам слід вміло аналізувати потоки інформації та розуміти, як вони можуть впливати на ціни криптовалют.

- сприйняття публічних висловлювань: Медійна грамотність також включає в себе вміння критично сприймати публічні висловлювання, зокрема ті, які стосуються криптовалют.

Переваги медійної грамотності в контексті криптовалют:

- зменшення впливу маніпуляцій: Інвестори, які володіють медійною грамотністю, менше схильні до маніпуляцій та впливу необґрунтованих чуток.

- формування об'єктивної позиції: Розуміння різних точок зору та аналіз різноманітності інформації допомагають інвесторам формувати об'єктивну позицію.

- проактивне реагування: Здатність швидко реагувати на новини та зміни в медійному ландшафті дозволяє інвесторам адаптуватися до нових умов ринку.

Можливі виклики та обмеження:

- інформаційне перевантаження: Завелика кількість інформації може призвести до інформаційного перевантаження, що робить важким визначення найважливіших та достовірних джерел.

- суб'єктивність оцінки: Різні інвестори можуть тлумачити інформацію по-різному, що може призвести до суб'єктивних рішень.

- залежність від доступу до інформації: Доступ до надійних джерел інформації може бути обмеженим для деяких інвесторів.

- ефективне використання соціальних мереж: Інвестори повинні володіти навичками аналізу інформації на соціальних мережах, де велика кількість дискусій та новин може впливати на перцепцію ринку.

- стратегії взаємодії із ЗМІ: Розуміння того, як взаємодія із засобами масової інформації може впливати на ринок та ціни криптовалют, є важливим для успішного інвестування.

Роль медійної грамотності в інвестуванні в криптовалюти:

- фільтрація інформації: Здатність розрізняти важливі новини від другорядних допомагає інвесторам приймати обґрунтовані рішення.
- уникнення психологічних впливів: Медійна грамотність допомагає інвесторам уникнути впливу чуток та суттєвої зміни настроїв ринку.
- адаптація до нових умов: Інвестори, які розуміють вплив змін в медійному просторі, можуть швидше адаптуватися до нових умов на ринку.
- підвищення рівня довіри: Обізнаність в сфері медійної грамотності допомагає підвищити рівень довіри до власних рішень та стратегій інвестування.
- ефективна комунікація: Інвестори можуть ефективно спілкуватися та ділитися інформацією з іншими членами громади, що сприяє обміну знаннями та досвідом.

Медійна грамотність є необхідною властивістю сучасного інвестора, оскільки швидкі та значущі зміни в інформаційному просторі можуть впливати на ринок криптовалют та визначати його динаміку. У цьому контексті вміння взаємодіяти з медіа та правильно оцінювати інформацію стає важливим фактором успішного інвестування.

3. Сприйняття ризиків інвесторами: Сприйняття ризиків та їх адекватне оцінювання є важливими аспектами захисту. Інвесторам важливо розуміти, що високі прибутки часто пов'язані з високим ризиком.

Сприйняття ризиків є вирішальним аспектом управління інвестиціями, особливо в контексті криптовалютних активів, які відзначаються високою волатильністю та нестабільністю. Розуміння, оцінка та ефективне управління ризиками грають ключову роль у формуванні стратегій інвесторів та досягненні їхніх фінансових цілей.

Основні аспекти сприйняття ризиків:

- розуміння інвестиційних ризиків: Інвестори повинні мати глибоке розуміння різних видів ризиків, пов'язаних із криптовалютами, таких як ринковий ризик, технічний ризик, регуляторний ризик тощо.
- оцінка та прогнозування ризиків: Здатність аналізувати поточні та потенційні ризики на ринку криптовалют та розуміти їхні можливі наслідки допомагає інвесторам ефективно прогнозувати та планувати свої дії.
- визначення рівня комфорту з ризиками: Кожний інвестор має свій власний рівень комфорту з ризиками. Розуміння та визначення цього рівня допомагає підібрати відповідні інвестиційні стратегії.
- управління ризиками в портфелі: Розподіл ризиків між різними активами та видами інвестицій дозволяє зменшити загальний ризик портфеля.

Переваги ефективного сприйняття ризиків:

- максимізація потенційних виграшів: Інвестори, які добре розуміють та приймають ризики, можуть бути більш готові до високодоходних можливостей на ринку криптовалют.

- зменшення психологічного стресу: Глибоке сприйняття ризиків допомагає інвесторам емоційно підготуватися до можливих втрат та уникнути неправомірних реакцій на ринкові коливання.

- ефективне планування: Інвестори можуть зробити ефективні рішення та плани, рахуючи ризики, що дозволяє досягати більш стійких результатів у довгостроковій перспективі.

Можливі виклики та обмеження:

- несприйняття ризиків: Деякі інвестори можуть недооцінювати ризики або ігнорувати їх, що може призвести до неправильних інвестиційних рішень.

- психологічні бар'єри: Емоції, такі як страх чи жадоба, можуть ускладнити раціональне сприйняття ризиків та впливати на рішення інвестора.

- невизначеність ринкових умов: Ринкова нестабільність та швидкі зміни умов можуть ускладнити точне сприйняття ризиків.

- створення резервного фонду: Інвестори, які ефективно сприймають ризики, можуть враховувати можливі втрати та створювати резервні фонди для захисту своїх портфелів у випадку несприятливих умов.

- адаптація до змін: Здатність адаптуватися до нових обставин та реагувати на зміни на ринку дозволяє інвесторам зберігати гнучкість та оптимізувати свої інвестиційні стратегії.

- визначення термінів інвестицій: Інвестори повинні чітко визначати терміни своїх інвестицій та рівень готовності до ризиків на певний період.

Роль сприйняття ризиків в контексті криптовалют:

- продуктивність інвестицій: Глибоке розуміння та правильне сприйняття ризиків допомагає інвесторам вибирати більш продуктивні та відповідні інвестиційні можливості.

- баланс між ризиком та винагородою: Сприйняття ризиків допомагає знайти оптимальний баланс між можливими вигодами та ризиками при виборі конкретних активів.

- зниження неоправданих ризиків: Інвестори, які усвідомлюють ризики, мають тенденцію уникати неоправданих ризиків та підвищують стійкість свого портфеля.

- підвищення фінансової свідомості: Сприйняття ризиків є частиною процесу фінансової освіти та розвитку, що допомагає інвесторам стати більш свідомими та обґрунтованими.

- ефективне планування на майбутнє: Інвестори, що враховують ризики, можуть краще планувати свою фінансову стратегію на майбутнє та уникати несподіваних фінансових труднощів.

Всебічне та обґрунтоване сприйняття ризиків є важливим фактором успішного управління інвестиціями, особливо в сфері криптовалют, де нестабільність та невизначеність є нормою.

Отже, забезпечення захисту криптовалютних активів вимагає інтегрованого підходу, який охоплює як ринкові, так і соціально-психологічні аспекти. Диверсифікація, технічний аналіз та використання стоп-лос замовлень є важливими інструментами ринкового захисту. Одночасно, інвесторам слід розвивати свою едукацію, вдосконалювати медійну грамотність та адекватно сприймати ризики для ефективного управління криптовалютними активами. Послідовне застосування цих методів може сприяти стабільності та успішному інвестуванню в цьому динамічному фінансовому середовищі.

2.3. Методи прогнозування ризиків на ринку криптовалютних активів

В сучасному фінансовому світі криптовалютні активи стають все більш привабливим об'єктом інвестицій через свою високу волатильність та потенційно високі прибутки. Однак разом із зростанням інтересу до цих активів зростає і рівень ризиків. Ефективне управління ризиками на ринку криптовалют вимагає використання високотехнологічних методів прогнозування.

Методи прогнозування ризиків:

1. Аналіз ринкової динаміки:

Аналіз ринкової динаміки на ринку криптовалют є ключовим елементом для розуміння та прогнозування ризиків. Цей метод включає в себе вивчення та оцінку рухів цін, обсягів торгів, тенденцій та інших ринкових параметрів. Врахування різних аспектів динаміки ринку дозволяє інвесторам розробляти обґрунтовані стратегії та приймати інвестиційні рішення на основі актуальних даних.

Основні компоненти аналізу ринкової динаміки в контексті криптовалют:

1) Цінова динаміка:

- історичний аналіз цін: Ретроспективний огляд цінових рухів допомагає виявити цінові патерни та тренди, які можуть бути показниками майбутньої динаміки.

- порівняння із секторами та конкурентами: Оцінка цінової динаміки у порівнянні з іншими криптовалютами та секторами дозволяє визначити конкурентні переваги чи недоліки конкретного активу.

2) Обсяги торгів:

- аналіз обсягів за періодами: Спостереження за обсягами торгів на різних часових періодах дозволяє виявляти інтерес інвесторів та можливі зміни в їхньому ставленні до активу.

- порівняння обсягів із змінами цін: Вивчення взаємозв'язку обсягів та змін цін допомагає виявляти потенційні точки входу чи виходу з позицій.

3) Тенденції та патерни:

- визначення основних тенденцій: Вивчення тривалості та стійкості основних тенденцій на ринку допомагає передбачити можливі напрямки руху цін.

- розпізнавання технічних патернів: Аналіз технічних патернів на графіках, таких як "голова і плечі", "прямокутник" чи "треугольник", може надати сигнали щодо майбутньої цінової динаміки.

4) Зовнішні фактори та новини:

- вплив зовнішніх подій: Врахування впливу новин, регуляторних рішень та інших зовнішніх факторів на ринкову динаміку.

- реакція на оголошення ключових подій: Спостереження за реакцією ринку на ключові події, такі як реліз нових продуктів чи партнерства, допомагає оцінити ставлення учасників ринку.

Методології аналізу ринкової динаміки можуть включати:

- лінійні та степеневі регресії: Для визначення та прогнозування цінових тенденцій.

- методи кластеризації та кореляції: Для виявлення груп схожих активів та взаємозв'язків між ними.

- синтез технічного та фундаментального аналізу: Комбінування технічного та фундаментального аналізу дозволяє отримати повніший образ ринкової ситуації.

- використання індикаторів та осциляторів: Спеціальні індикатори, такі як RSI, MACD чи Bollinger Bands, використовуються для виявлення періодів перекупленості чи перепроданості активу, що може бути показником майбутніх ризиків.

Переваги аналізу ринкової динаміки:

1) обґрунтоване прийняття рішень: Аналіз ринкової динаміки допомагає інвесторам приймати обґрунтовані рішення на основі реальних та актуальних даних.

2) вчасна реакція на зміни: Систематичний аналіз дозволяє вчасно виявляти та реагувати на зміни у ринкових умовах, зменшуючи ризики.

3) зростання ефективності торгівлі: Інвестори, які ретельно вивчають ринкову динаміку, можуть вдосконалити свої стратегії та підвищити ефективність торгівлі.

Обмеження та виклики:

1) висока волатильність крипторинку: Нестабільність цін на криптовалютному ринку може ускладнювати точне прогнозування.

2) невизначеність регуляторних аспектів: Зміни в регуляторному середовищі можуть внести непередбачувані елементи у ринкову динаміку.

3) психологічні аспекти ринку: Ринкова поведінка може бути під впливом емоцій та психологічних факторів, що ускладнює точний аналіз.

Аналіз ринкової динаміки є ключовим елементом в інвестиційному процесі, де криптовалютний ринок вирізняється своєю особливою природою та високою волатильністю. Застосування різноманітних методів аналізу, врахування змінливості ринкових умов, та здатність вчасно реагувати на події дозволяє інвесторам ефективно керувати ризиками та максимізувати можливі прибутки.

2. Моделі машинного навчання:

Використання моделей машинного навчання на ринку криптовалют дозволяє інвесторам отримати значний інструментарій для прогнозування ризиків та прийняття обґрунтованих інвестиційних рішень. Машинне навчання базується на здатності комп'ютерних систем адаптуватися та вдосконалювати свої алгоритми на основі даних.

Основні методи та моделі машинного навчання для прогнозування ризиків на ринку криптовалют:

1) Лінійна регресія:

Лінійна регресія використовує лінійні залежності між вхідними та вихідними змінними для прогнозування значень. Застосовується для моделювання та прогнозування цінових та ринкових тенденцій.

2) Нейронні мережі:

Моделі, які імітують структуру та функції нейронів у мозку, призначені для виявлення складних нелінійних залежностей. Ефективні для аналізу складних ринкових динамік та виявлення неочікуваних патернів.

3) Дерева рішень:

Моделі, які розглядають різні можливі шляхи прийняття рішень та дозволяють визначити оптимальні стратегії. Використовуються для прогнозування ризиків та виявлення ключових факторів впливу.

4) Метод опорних векторів (SVM):

SVM визначає оптимальну границю прийняття рішень для класифікації даних. Використовується для виявлення трендів та класифікації ризиків на ринку.

5) Зграйне навчання:

Модель, яка моделює поведінку колективу та використовує інтелект групи для прийняття рішень. Використовується для вивчення та адаптації до змін у колективному ринковому виборі.

Переваги та виклики моделей машинного навчання в прогнозуванні ризиків:

Переваги:

- Здатність адаптуватися до змін в ринкових умовах.
- Обробка великого обсягу даних та швидкість прийняття рішень.
- Здатність виявляти складні нелінійні залежності та патерни.

Виклики:

- Потреба в великій кількості даних для навчання нейронних мереж.
- Схильність до перенавчання та непереносимість результатів між різними ринковими умовами.
- Складність в поясненні прийнятих рішень («чорна скринька»).

Застосування моделей машинного навчання в практиці:

1) Прогнозування трендів: Використання нейронних мереж та дерев рішень для виявлення та прогнозування трендів на ринку криптовалют. Моделі можуть реагувати на зміни у ринковій динаміці та вказувати на ймовірні ризики.

2) Аналіз соціальних мереж: Використання зграйного навчання для аналізу великої кількості даних з соціальних мереж. Це дозволяє виявляти суспільні настрої, тренди та новітні ринкові інсайти.

3) Класифікація ризиків: Застосування методу опорних векторів для класифікації ризиків на ринку. Модель може визначати, до якої категорії належить конкретний ризик та допомагати в прийнятті стратегічних рішень.

4) Прогнозування волатильності: Використання лінійної регресії для прогнозування рівня волатильності на ринку криптовалют. Це дозволяє інвесторам адаптуватися до змін в ринковій атмосфері та раціонально управляти портфелем.

Розгляд індивідуальних моделей:

1) Лінійна регресія:

Переваги:

- Простота в розумінні та впровадженні.

- Ефективність для лінійних залежностей у даних.

Виклики:

- Недостатнє урахування складних нелінійних патернів.

2) Нейронні мережі:

Переваги:

- Здатність виявляти складні залежності та адаптуватися до різноманітних даних.

- Великий потенціал для точного прогнозування.

Виклики:

- Потреба в великій кількості даних та ресурсів для навчання.

3) Дерева рішень:

Переваги:

- Здатність моделювати складні стратегії прийняття рішень.

- Легкість інтерпретації результатів.

Виклики:

- Недостатнє урахування взаємодій між різними змінними.

4) Метод опорних векторів (SVM):

Переваги:

- Ефективність в роботі зі складними нелінійними даними.

- Добра узагальнююча здатність.

Виклики:

- Високі вимоги до обчислювальних ресурсів.

Моделі машинного навчання стають невід'ємною частиною інструментарію для прогнозування ризиків на ринку криптовалют. Вони дозволяють ефективно використовувати велику кількість даних та виявляти складні залежності, що допомагає інвесторам приймати обґрунтовані рішення в умовах високої волатильності та невизначеності.

3. Сентимент-аналіз:

Сентимент-аналіз, також відомий як аналіз настроїв, представляє собою метод вивчення та визначення настроїв, емоцій та ставлень людей за допомогою автоматизованого аналізу тексту. У контексті ринку криптовалют, сентимент-аналіз використовується для визначення того, як спільні настрої та емоції можуть впливати на ринкову динаміку.

Ключові аспекти сентимент-аналізу в криптосфері:

1) Аналіз соціальних мереж:

Сентимент-аналіз часто застосовується до коментарів та повідомлень у соціальних мережах, форумах та новинних порталах. Автоматична обробка великого обсягу тексту дозволяє виявляти загальні настрої громадськості.

2) Оцінка ставлень та реакцій ринку:

- Сентимент-аналіз може служити індикатором того, як ринок реагує на певні події. Наприклад, анонс нового продукту чи зміни в регуляторному середовищі може суттєво впливати на сентимент.

3) Прогнозування ринкових трендів:

- Штучний інтелект і алгоритми машинного навчання дозволяють прогнозувати можливі ризики та напрямки ринкових трендів на основі аналізу сентименту.

4) Взаємодія з технічним аналізом:

- Сентимент-аналіз може бути використаний для підтримки технічного аналізу, дозволяючи трейдерам отримувати більш повні та збалансовані прогнози.

Методи та інструменти сентимент-аналізу:

1) Машинне навчання: Застосування моделей машинного навчання для класифікації текстів за тональністю та визначення сентименту. Нейронні мережі та методи опорних векторів є популярними.

2) Аналіз глибини тексту: Врахування не лише словесного змісту тексту, а й його контексту та семантичного змісту. Використання алгоритмів обробки природної мови (NLP) дозволяє краще розуміти сутність текстової інформації.

3) Аналіз графів: Використання графових структур для визначення взаємозв'язків між різними елементами ринкового сентименту, такими як користувачі соціальних мереж або великі групи трейдерів.

Виклики та Обмеження:

1) Неоднозначність тексту: Неоднозначність та многозначність текстового матеріалу може створювати труднощі у правильному визначенні настроїв.

2) Зміна смислу в контексті: Зміна смислу в залежності від контексту може призводити до неточностей у розумінні сентименту, особливо у випадках вживання жаргону чи сленгу.

3) Вплив фейків та маніпуляцій: Вплив фейкових новин та маніпуляцій на соціальних мережах може спричиняти спотворення результатів сентимент-аналізу.

4) Відсутність контекстуального розуміння: Деякі методи сентимент-аналізу можуть бути обмеженими у розумінні контексту, що може призводити до неточних висновків.

Застосування сентимент-аналізу в практиці:

1) Моніторинг новин та соціальних мереж: Використання інструментів сентимент-аналізу для моніторингу та аналізу новинних порталів, форумів та соціальних мереж для визначення настроїв користувачів.

2) Прогнозування ринкових змін: Використання сентимент-аналізу для прогнозування можливих змін у ринкових умовах та цінових трендах.

3) Підтримка технічного аналізу: Інтеграція результатів сентимент-аналізу в технічний аналіз для отримання комплексних прогнозів та рекомендацій.

4) Управління ризиками: Використання сентимент-аналізу для розуміння емоційного стану ринку та прийняття рішень з урахуванням ризиків.

Сентимент-аналіз є суттєвим інструментом для інвесторів та трейдерів на ринку криптовалют, допомагаючи їм краще розуміти громадські настрої та емоції, які можуть впливати на рішення та цінову динаміку. Однак, важливо враховувати обмеження та виклики цього методу, особливо пов'язані з неоднозначністю мовлення та впливом фейкових новин. Використання сентимент-аналізу разом з іншими методами аналізу дозволяє створити більш об'єктивне та комплексне уявлення про ринкові умови.

4. Моделювання стрес-тестів:

Моделювання стрес-тестів у контексті криптовалютного ринку представляє собою метод, що дозволяє оцінити реакцію фінансових систем та інвестиційних портфелів на надзвичайні події та стресові умови. Цей підхід є важливим елементом управління ризиками та роботи з фінансовими інструментами, оскільки він дозволяє передбачити вплив небезпечних сценаріїв на портфель і здійснити відповідні заходи для зменшення можливих втрат.

Основні аспекти моделювання стрес-тестів на ринку криптовалют:

1) Оцінка ризиків та вразливостей: Моделювання стрес-тестів дозволяє ідентифікувати можливі ризики та вразливості в інвестиційних портфелях під впливом стресових сценаріїв, таких як різкі зміни цін, великі виведення коштів, чи технічні невдачі.

2) Сценарії системних змін: Розробка сценаріїв системних змін, таких як різке зростання чи спад ринкової активності, атаки на мережу чи зміни в регулюванні, для оцінки впливу на криптовалютні ринки.

3) Аналіз ліквідності: Визначення рівня ліквідності та оцінка, як вона може змінюватися під час стресових сценаріїв, що допомагає уникнути проблем з виведенням коштів та непередбачуваними витратами.

Методи та інструменти моделювання стрес-тестів:

1) Математичні моделі ризиків: Використання математичних моделей для визначення можливих втрат у залежності від різних факторів та змінних, таких як ціни, ліквідність та волатильність.

2) Сценарійна аналітика: Розробка та аналіз різних сценаріїв для визначення того, як інвестиційний портфель реагує на стресові умови, такі як масштабні цінові коливання або великі виведення активів.

3) Симуляції МонтеКарло: Використання симуляцій МонтеКарло для моделювання тисячі можливих сценаріїв та оцінювання ризиків та можливих втрат.

Практичне застосування моделювання стрес-тестів:

1) Управління ризиками: Стрес-тестінг дозволяє менеджерам портфеля та інвесторам зрозуміти, як їхні інвестиції можуть вести себе в екстремальних умовах та приймати відповідні заходи для зменшення ризиків.

2) Розробка стратегій: Моделювання стрес-тестів допомагає інвесторам розробляти стратегії, які враховують можливі стресові сценарії та максимізують можливість виживання в них.

3) Внутрішній та зовнішній аудит: Використання стрес-тестів для проведення аудитів фінансових установ та інвестиційних компаній, щоб переконатися, що вони готові до різних фінансових викликів.

4) Розробка регуляторної політики: Стрес-тестінг може бути важливим елементом розробки та вдосконалення регуляторної політики для фінансових установ та ринків.

Виклики та обмеження:

1) Недостатня інформація: Моделювання стрес-тестів залежить від точності та повноти вхідних даних. Недостатня інформація може призвести до неточностей у прогнозуванні.

2) Складність сценаріїв: Розробка реалістичних та комплексних стрес-сценаріїв може бути викликом, особливо у врахуванні непередбачуваних подій.

3) Неоднорідність ринків: Різнорідність ринків та активів може ускладнити розробку загальних стрес-тестів, оскільки кожен ринок має свої унікальні характеристики.

Застосування сучасних технологій:

1) Штучний інтелект та машинне навчання: Використання алгоритмів штучного інтелекту для автоматизації процесу стрес-тестів та аналізу великої кількості даних.

2) Блокчейн та смарт-контракти: Використання технологій блокчейн та смарт-контрактів для автоматизації виконання стрес-тестів та забезпечення прозорості результатів.

3) Системи реального часу: Застосування систем реального часу для моніторингу ринкових умов та миттєвого реагування на стресові сценарії.

Моделювання стрес-тестів виявляється необхідним елементом управління ризиками на криптовалютних ринках, де волатильність та невизначеність є невід'ємними частинами. Використання різноманітних методів, включаючи математичні моделі, сценарійну аналітику та симуляції МонтеКарло, дозволяє оцінити та підготуватися до можливих ризикових ситуацій. Застосування сучасних технологій, таких як штучний інтелект та блокчейн, допомагає покращити точність та ефективність цих стратегій.

Методи прогнозування ризиків на ринку криптовалютних активів є критичними для забезпечення стійкості та ефективного управління портфелем. Комбінація традиційних аналітичних інструментів із сучасними технологіями машинного навчання створює комплексні методи, які можуть допомогти інвесторам адекватно реагувати на непередбачувані обставини та мінімізувати можливі ризики.

РОЗДІЛ 3
СТРАТЕГІЯ ЗАХИСТУ КРИПТОВАЛЮТНИХ АКТВІВ НА ПРИКЛАДІ ЗАХИСТУ ГАМАНЦІВ

3.1. Оцінка ефективності існуючих стратегій захисту криптовалютних активів

У світі стрімкого розвитку криптовалют та цифрових активів зростає імператив ефективного захисту цих цінних ресурсів від різноманітних кіберзагроз. Особливу увагу приділяється захисту гаманців, як ключового елементу для зберігання приватних ключів та доступу до криптовалютних активів.

В контексті загального захисту криптовалютних активів, оцінка ефективності існуючих стратегій захисту криптовалютних активів стає фокусом уваги, де проводиться глибока аналітична оцінка різних стратегій захисту. Надзвичайна важливість цього аспекту полягає в тому, щоб визначити оптимальні та надійні методи збереження та захисту цифрових активів в умовах постійно зростаючого рівня кіберзагроз та інновацій у сфері криптовалют.

Гаманець є ключовим елементом у зберіганні криптовалют, і від його безпеки залежить надійність і цілісність цифрового майна користувача.

Розглянемо ефективність різноманітних стратегій, звертаючи увагу на технічні та соціальні аспекти, які визначають безпеку гаманців та взагалі цифрового власності:

1. Технічні аспекти захисту гаманців

У сучасному цифровому середовищі, де криптовалютні активи відіграють важливу роль, безпека зберігання цих активів стає вирішальним аспектом. Однією з ключових складових цієї безпеки є захист гаманців, які зберігають приватні ключі користувачів і забезпечують їх доступ до власних цифрових власностей.

Вивчення технічних аспектів захисту гаманців включає в себе аналіз різноманітних технологічних рішень, спрямованих на максимізацію безпеки приватних ключів та запобігання несанкціонованому доступу. Один із підходів полягає у використанні апаратного забезпечення для ізольованого зберігання ключової інформації. Апаратні гаманці, які використовуються для цієї мети, надають додатковий рівень захисту шляхом створення ізольованого середовища для генерації підписів та зберігання ключів.

Далі, у вивченні технічних аспектів звертається увага на впровадження двофакторної аутентифікації як засобу збільшення безпеки. Цей підхід вимагає дві різні форми ідентифікації для підтвердження особи користувача, забезпечуючи тим самим більш високий рівень авторизації.

Окрім того, у науковому вивченні розглядаються використані алгоритми шифрування для захисту конфіденційності приватних ключів та інших чутливих даних. Проводиться аналіз їхньої стійкості та відповідності сучасним стандартам безпеки.

Зокрема, досліджується роль технічних засобів захисту, таких як відділення гаманця від мережі для запобігання онлайн-атак, а також використання механізмів безпеки для виявлення та запобігання можливим атакам на гаманці.

Таким чином, науковий аналіз технічних аспектів захисту гаманців має на меті визначити оптимальні та ефективні стратегії, спрямовані на максимальне забезпечення безпеки для криптовалютних активів користувачів в умовах постійно зростаючого ризику кіберзлочинності.

Позначаючи значущість технічних заходів захисту гаманців, варто взяти до уваги інші важливі аспекти, що стосуються безпеки цифрових активів. Одним із таких аспектів є використання механізмів автоматизованого виявлення підозрілих або несанкціонованих дій, що може бути реалізоване через системи виявлення вторгнень.

Також вивчається можливість ефективного відділення гаманця від мережі для зменшення ризику онлайн-атак та злому. Цей підхід сприяє

створенню додаткового бар'єру для потенційних загроз, які можуть виникнути в онлайн середовищі.

Окрім того, при аналізі технічних аспектів важливо враховувати не лише поточний стан технологічних рішень, але і їхню придатність для майбутніх викликів та еволюції загроз кібербезпеки. Забезпечення масштабованої та стійкої архітектури захисту важливо для довгострокової безпеки цифрових активів.

Загальний науковий підхід до вивчення технічних аспектів захисту гаманців полягає в розумінні взаємодії різних компонентів, їхніх переваг та обмежень. Такий підхід дозволяє визначити оптимальні стратегії та інтегровані заходи, спрямовані на забезпечення повноцінної та надійної безпеки криптовалютних гаманців.

Отже, науковий аналіз технічних аспектів захисту гаманців є важливим етапом для розробки імплементованих та ефективних стратегій кібербезпеки в контексті зростаючого виклику забезпечення безпеки криптовалютних активів в цифровому віці.

2. Соціальна інженерія в захисті гаманців

Сучасний цифровий ландшафт надто залежить від криптовалют, які визначають новий етап фінансових та економічних відносин. Захист цих криптовалютних активів є надзвичайно важливою задачею, і в цьому контексті соціальна інженерія виступає як значущий аспект забезпечення кібербезпеки.

Соціальна інженерія, як концепція, охоплює широкий спектр методів, які зловмисники використовують для впливу на людей і отримання несанкціонованого доступу до конфіденційної інформації. У контексті захисту гаманців, це може включати в себе різноманітні форми соціального маніпулювання з метою отримання доступу до приватних ключів або інших конфіденційних даних.

Загрози соціальної інженерії можуть включати фішингові атаки, в яких атакуючі вдаються в особи чи організації, щоб отримати конфіденційну інформацію. Вони можуть виглядати як надійні джерела або використовувати

маніпулятивні техніки, щоб обманити користувачів і навіть впровадити їх до розкриття своїх приватних ключів.

До інших методів соціальної інженерії можна віднести імітацію авторитетних осіб чи сервісів, щоб спонукати користувачів до виконання дій, які можуть стати загрозою для безпеки їхніх гаманців. Зловмисники можуть використовувати психологічні прийоми для створення довіри та викликання необдуманих дій у потенційних жертв.

Застосування соціальної інженерії в захисті гаманців вимагає не лише технічних заходів, але і освітніх програм, спрямованих на підвищення свідомості користувачів щодо потенційних загроз та методів їх запобігання. Врахування соціальних аспектів у стратегіях захисту стає невід'ємною частиною багатогранного підходу до кібербезпеки криптовалютних активів.

Особливу увагу слід звертати на те, щоб покращити навички розпізнавання соціально-інженерних атак серед користувачів. Дієві методи включають проведення інформаційних кампаній та тренінгів, спрямованих на розпізнавання підозрілих повідомлень та ситуацій, які можуть призвести до небезпечних дій.

Окрім того, застосування технологій штучного інтелекту для виявлення аномалій та надзвичайних патернів у поведінці користувачів може забезпечити додатковий рівень захисту. Алгоритми машинного навчання можуть виявляти незвичайні взаємодії та попереджати користувачів про можливі загрози.

Також важливо розглядати соціальну інженерію не лише як загрозу, але і як можливість покращити системи безпеки. Вивчення таких аспектів дозволяє розробляти адаптивні стратегії, які беруть до уваги людський фактор і впроваджують технологічні і організаційні засоби для запобігання соціальним інженерним атакам.

Усе це вказує на необхідність інтеграції соціальної інженерії в загальний контекст стратегій кібербезпеки гаманців. Це вимагає колективних зусиль технічних спеціалістів, психологів та освітніх експертів для створення

повноцінної та ефективної системи захисту, що враховує не лише технічні аспекти, але і людський фактор в кіберпросторі.

Досягнення повноцінного захисту від соціально-інженерних загроз включає в себе створення ефективної системи звільнення від ризиків, яка враховує технічні та психосоціальні аспекти. Організації та індивіди повинні розвивати не тільки технічні навички, але і здатність критичного мислення та аналізу при взаємодії з інтернет-ресурсами та комунікацією в цифровому середовищі.

Важливо також враховувати динаміку соціально-інженерних атак і постійно адаптувати заходи безпеки для виявлення нових форм маніпуляцій та афішування загроз. Впровадження систем виявлення аномалій та інтелектуальних технологій для аналізу поведінки користувачів може значно полегшити виявлення потенційних атак.

Необхідно покладати особливий акцент на освіту та підвищення обізнаності користувачів у сфері кібербезпеки. Ініціативи з проведення тренінгів та навчання можуть підняти рівень обізнаності щодо ризиків соціально-інженерних атак та зробити користувачів менш вразливими до маніпуляцій.

Усі ці аспекти свідчать про складність і багатогранність проблеми соціальної інженерії в захисті гаманців. Інтеграція технічних та соціальних аспектів в рамках комплексних стратегій захисту може стати вирішальним етапом для ефективного захисту від сучасних кіберзагроз. Однак це вимагає постійного вдосконалення та адаптації стратегій відповідно до зростаючих ризиків та еволюції технологій.

3. Заходи безпеки на рівні користувача

В сучасному цифровому ландшафті, в якому користувачі взаємодіють із різноманітними технологіями та сервісами, безпека на рівні користувача стає критично важливою.

Значення безпеки на рівні користувача необхідно розглядати в контексті розширюваної кількості кіберзагроз та кібератак. Користувачі зіштовхуються

із загрозами, які можуть включати фішингові атаки, шкідливе програмне забезпечення, а також крадіжку особистих даних. Забезпечення особистої інформаційної безпеки стає викликом, оскільки техніки атак постійно еволюціонують.

У рамках цього дослідження розглядаються різноманітні аспекти безпеки на рівні користувача, починаючи від освіти та свідомості, які є важливими елементами запобігання соціальній інженерії та фішинговим атакам. Важливо виробляти у користувачів навички розпізнавання потенційно небезпечних ситуацій та поведінки в Інтернеті.

Застосування технічних заходів, таких як антивірусне програмне забезпечення та файрволи, розглядається як інший важливий аспект безпеки на рівні користувача. Аналізуються методи виявлення та захисту від шкідливого програмного забезпечення, оскільки вони можуть потенційно завдати значних збитків для користувачів.

Також вивчається роль безпечних практик в користувальницькому поведінці, таких як регулярне оновлення програм та операційних систем, складні паролі та безпечне підключення до мереж. Всі ці аспекти призначені для максимізації безпеки та захисту особистих даних на рівні кінцевого користувача.

Особливу увагу слід приділити також питанням використання та зберігання паролів, які є важливим елементом безпеки. Аналізуються сучасні методи автентифікації, такі як двофакторна аутентифікація, що може значно підвищити рівень захисту особистих облікових записів.

Дослідження також ставить у центральний план питання кібергігієни – правильної організації та управління своїми цифровими слідами. Користувачам рекомендується вдосконалювати свої навички використання інтернет-послуг, контролювати доступ до особистих даних та регулярно аудитувати їхні налаштування з метою мінімізації ризиків.

Зазначимо, що в рамках безпеки на рівні користувача індивідуальна відповідальність відіграє ключову роль. Поширення інформації про загрози та

вчасна реакція на можливі атаки є важливим елементом успішного захисту. Забезпечення освіти та підтримки для користувачів стає основним інструментом у формуванні культури кібербезпеки.

У великій мірі, індивідуальна безпека користувача також пов'язана з його здатністю визначати соціальні інженерні атаки та уникати психологічних впливів, що можуть призвести до розкриття конфіденційної інформації. У цьому контексті, дослідження психосоціальних аспектів безпеки користувача визначається як важливий напрямок для подальших досліджень.

Таким чином, вивчення заходів безпеки на рівні користувача в контексті сучасних викликів цифрового світу виявляється комплексним та багатогранним завданням, яке вимагає інтеграції технічних, організаційних та освітніх підходів.

4. Порівняльний аналіз стратегій захисту

Сучасний дигітальний ландшафт вимагає ретельного аналізу та вивчення стратегій захисту як важливого аспекту кібербезпеки. Цей науковий реферат спрямований на вивчення та порівняльний аналіз різноманітних стратегій захисту, спрямованих на забезпечення інформаційної безпеки в цифровому середовищі.

Однією із ключових аспектів є технічний підхід до захисту. В даному дослідженні аналізуються технологічні рішення, такі як використання антивірусного програмного забезпечення, файрволів, та систем виявлення вторгнень. Оцінка ефективності технічних стратегій базується на їхній здатності виявляти та запобігати різноманітним кіберзагрозам.

Однак, важливо враховувати не лише технічні аспекти. Стратегії соціальної інженерії та психологічні аспекти захисту стають все більш суттєвими в умовах зростаючого числа атак, спрямованих на людський фактор. Порівняння технічних і соціальних стратегій дозволяє визначити їхню відмінність та можливості взаємодії для створення комплексних заходів безпеки.

У контексті стратегій захисту важливо вивчати інноваційні підходи, такі як використання штучного інтелекту та машинного навчання. Аналіз розвитку цих технологій дозволяє передбачити їхню роль у майбутньому та їхню спроможність пристосовуватися до зростаючих загроз.

Організаційні стратегії та політики також займають важливе місце у системі захисту. Вивчення внутрішніх процесів, стандартів безпеки, та практик управління ризиками розкриває можливості для створення більшої стійкості та цілісності інформаційних систем.

Таблиця 3.1

Порівняльний аналіз стратегій захисту

Стратегії захисту		Переваги/Недоліки
Технічні стратегії захисту	1. Використання антивірусного програмного забезпечення (АПЗ):	Переваги: Здатність виявляти та блокувати загрози шкідливого програмного забезпечення. Недоліки: Обмежена ефективність у виявленні нових, невідомих загроз; неспроможність захистити від соціальних аспектів, таких як фішинг.
	2. Фаєрволи та системи виявлення вторгнень (IDS/IPS):	Переваги: Забезпечують моніторинг мережі та виявлення аномалій. Недоліки: Можливі ложні спрацювання; обмежена здатність реагувати на нові, розширені загрози; не враховують соціальні аспекти.
	3. Шифрування даних	Переваги: Забезпечує конфіденційність інформації; ускладнює доступ для несанкціонованих осіб. Недоліки: Можливість втрати доступу до даних при втраті ключів; потребує великої обчислювальної потужності.
Соціальні стратегії захисту	1. Освіта та навчання	Переваги: Підвищення свідомості користувачів; розпізнавання соціальних атак. Недоліки: Низька ефективність при взаємодії з високохитрими соціальними інженерами; вимагає постійного оновлення.
	2. Двофакторна аутентифікація (2FA):	Переваги: Додатковий рівень безпеки через використання двох елементів для підтвердження ідентичності. Недоліки: Потребує додаткових зусиль від користувача; можливість атак через соціальне інженерію.

	3. Спільнота безпеки	Переваги: Обмін інформацією та попередження про загрози спільнотою користувачів. Недоліки: Залежність від активності спільноти; можливість розповсюдження неперевіреної інформації.
Комплексний підхід та перспективи		Переваги: Інтеграція технічних та соціальних стратегій створює більш високий рівень безпеки; здатність адаптуватися до нових загроз. Недоліки: Вимагає координації різних заходів; необхідність постійного моніторингу та оновлення стратегій.

Технічні та соціальні стратегії захисту, взяті разом, формують комплексний підхід до безпеки криптовалютних активів. Технічні заходи надають технічну оборону, в той час як соціальні стратегії акцентують увагу на користувачах та їхній поведінці. Ефективність такого підходу залежить від правильної інтеграції та постійного вдосконалення стратегій з урахуванням динаміки загроз та технологічних інновацій.

Оцінка ефективності існуючих стратегій захисту криптовалютних активів підкреслює важливість комплексного підходу до забезпечення безпеки в цифровому середовищі. Розгляд технічних та соціальних стратегій підкреслив їхні переваги та недоліки, а також важливість їхньої взаємодії.

Загалом, розвиток стратегій захисту криптовалютних активів є постійним завданням, яке вимагає уваги до інновацій, взаємодії різних сторін, та адаптації до найновіших технологічних та соціальних викликів.

3.2. Оптимізаційна (імітаційна) модель стратегії захисту криптовалютних активів - постановка задачі та її розв’язок

В умовах постійного розвитку криптовалют та зростаючої кількості кіберзагроз, захист криптовалютних активів стає завданням надзвичайно важливим для забезпечення конфіденційності та цілісності фінансових

ресурсів. Відповідно, виникає необхідність розробки оптимізаційних (імітаційних) моделей стратегій захисту.

Захист гаманців, як елемента, що зберігає криптовалютні ключі, є критичним завданням у контексті забезпечення безпеки криптовалют. Постановка задачі передбачає наступні етапи:

1. Визначення загроз та вразливостей: Аналіз можливих загроз, таких як атаки на гаманці через технічні вразливості або соціальні методи.

2. Формулювання цільової функції: Створення математичної цільової функції, яка враховує ефективність стратегії та зменшення ризиків.

3. Визначення параметрів моделі: Обрання ключових параметрів, таких як вартість розвитку технічних рішень, тривалість навчання персоналу, рівень освіти користувачів гаманців.

4. Створення імітаційної моделі: Розробка імітаційної моделі взаємодії технічних та соціальних стратегій захисту гаманців.

5. Вибір оптимальних параметрів: Використання алгоритмів оптимізації для визначення оптимальних параметрів стратегії захисту.

Розробка імітаційної моделі взаємодії технічних та соціальних стратегій захисту гаманців передбачає створення спрощеної віртуальної системи, яка відтворює ключові аспекти реального світу. Загальний план для такої моделі:

1. Визначення системних агентів:

- Технічні системні агенти: Представляють технічні засоби захисту, такі як антивірусне програмне забезпечення, шифрування, системи виявлення вторгнень.

- Соціальні системні агенти: Відображають людей та їхню поведінку, включаючи рівень обізнаності, освіту та усвідомленість щодо кібербезпеки.

2. Моделювання технічних засобів захисту:

- Властивості: Визначення характеристик технічних засобів, таких як ефективність виявлення загроз, швидкість реакції на нові атаки, витрати на утримання.

- Поведінка: Симуляція функціоналу антивірусних програм, систем шифрування, та інших технічних засобів захисту.

3. Моделювання людської поведінки:

- Рівень обізнаності: Випадкове або згідно із статистикою визначення рівня обізнаності користувачів щодо кібербезпеки.

- Реакція на соціальні атаки: Моделювання відповіді людини на фішингові атаки, соціальну інженерію та інші соціальні загрози.

4. Взаємодія між агентами:

- Комунікація: Моделювання обміну інформацією між технічними та соціальними системними агентами.

- Вплив технічних засобів на людей та навпаки: Визначення, як використання технічних засобів впливає на поведінку людей та навпаки.

5. Збір та аналіз даних:

- Статистика: Збір статистичних даних щодо ефективності технічних та соціальних стратегій.

- Відстеження подій: Запис подій та реакцій системи на різні загрози.

6. Оцінка ефективності:

- Критерії оцінки: Визначення критеріїв, таких як рівень захищеності, витрати, прийняття користувачами стратегій.

- Аналіз результатів: Висновки щодо ефективності взаємодії технічних та соціальних стратегій.

7. Апробація та калібрування:

- Порівняння з реальним світом: Порівняння результатів моделювання з реальними статистиками та подіями.

- Вдосконалення моделі: Внесення коректив та вдосконалень до імітаційної моделі на основі аналізу порівнянь та результатів апробації.

Розробка імітаційної моделі взаємодії технічних та соціальних стратегій захисту гаманців є важливим кроком у напрямку розуміння та вдосконалення заходів кібербезпеки. Ця модель дозволяє оцінювати вплив різних факторів на

ефективність стратегій та прогнозувати їхню поведінку в умовах зростаючих загроз.

Моделювання взаємодії технічних та соціальних аспектів забезпечення безпеки гаманців не лише дозволяє визначити оптимальні стратегії, але й надає можливість експериментувати та вдосконалювати підходи до кібербезпеки в цілому. Важливим аспектом є можливість адаптації моделі до нових загроз та технологічних інновацій, щоб завжди мати актуальні та ефективні стратегії.

Враховуючи динаміку кіберзагроз та необхідність комплексного підходу до захисту, імітаційна модель взаємодії стає потужним інструментом для кібербезпеки, який дозволяє пристосовуватися до змін у кіберпросторі та навколишньому соціальному середовищі.

Імітаційна модель взаємодії технічних та соціальних стратегій захисту гаманців не лише відтворює складні взаємодії в цифровому середовищі, але й виступає важливим інструментом для тестування та вдосконалення стратегій безпеки. Результати моделювання можуть слугувати основою для розробки практичних рекомендацій та стратегій кіберзахисту гаманців у реальному світі.

Поєднання технічних та соціальних аспектів у моделі враховує комплексність загроз та дозволяє краще розуміти вплив людського фактору на кібербезпеку. Успішна взаємодія цих двох складових може забезпечити сильний та довгостроковий захист від різноманітних атак та загроз.

Подальший розвиток імітаційних моделей такого типу сприятиме розумінню ефективних стратегій захисту не лише для гаманців, а й для інших ключових елементів криптовалютної інфраструктури. Високоточні та адаптивні моделі є важливим кроком у напрямку підвищення рівня кібербезпеки в умовах постійної зміни кіберзагроз та технологічного прогресу.

Таким чином, імітаційні моделі взаємодії технічних та соціальних стратегій є потужним інструментом для вивчення та оптимізації заходів з

кіберзахисту, а їхнє вдосконалення є ключовим завданням для створення ефективної системи кібербезпеки в сучасному цифровому світі.

3.3. Перспективи розвитку ринку криптовалютних активів з урахуванням розроблених стратегій їх захисту

В умовах стрімкого технологічного прогресу та зростаючої зацікавленості глобального суспільства у цифрових фінансах ринок криптовалютних активів набуває все більшого значення. Перед ним стоять великі можливості та виклики, зокрема у сфері кібербезпеки.

1. Зростання значення ринку криптовалютних активів

У сучасному фінансовому ландшафті ринок криптовалютних активів активно та неперервно збільшує свою площину впливу. Цей ринок стає об'єктом значної уваги як індивідуальних інвесторів, що включають фахівців та приватних осіб, так і великих корпорацій, які розглядають цифрові активи як стратегічний елемент свого портфеля.

Зростання інтересу до криптовалютних активів може бути пояснене рядом факторів. По-перше, вони пропонують альтернативу традиційним фінансовим інструментам, що привертає тих, хто шукає нові можливості для інвестування та диверсифікації свого портфеля. По-друге, технологія блокчейн, на якій базується більшість криптовалют, викликає серйозний інтерес своєю децентралізованістю та потенцією для революційних змін у різних галузях.

Забезпечення безпеки цих криптовалютних активів нині є необхідним завданням, оскільки вони стикаються з численними викликами через свою динамічність та високий рівень чутливості до кіберзагроз. Зокрема, враховуючи потенційно великі обсяги капіталу, які обертаються на цьому ринку, забезпечення конфіденційності, цілісності та доступності криптовалют стає критично важливим, особливо в умовах постійно зростаючого рівня кіберзагроз та швидко змінюючогося кіберпростору.

Зростання інтересу інвесторів та корпорацій викликає важливі питання щодо безпеки криптовалютних активів. Зважаючи на їхню велику вартість і потенційно великі втрати в разі кібератак або інших загроз, необхідність ефективного та надійного захисту стає безперечною.

Динамічність природи ринку криптовалют визначається швидкими коливаннями цін, нововведеннями та постійним розвитком технологій. Це вимагає адаптивності та оперативної реакції владарів стратегій захисту для ефективного опитування нових викликів та загроз.

Висока чутливість криптовалютних активів до кіберзагроз обумовлена їхнім цифровим характером та використанням технологій, які можуть бути вразливими перед різними видами атак. Це включає, але не обмежується, кібервторгівлю, атаки на блокчейн-технології, фішинг, атаки на обмінні платформи та інші.

Забезпечення кібербезпеки на ринку криптовалютних активів стає фундаментальним елементом для збереження довіри та стабільного функціонування цього ринку. Інвестори та корпорації, які виявляють високий рівень довіри до захисту своїх криптовалютних активів, можуть бути більш схильними активно взаємодіяти з цим ринком.

У світлі цих викликів важливо розвивати та впроваджувати сучасні стратегії кібербезпеки, що охоплюють як технічні, так і соціальні аспекти. Такий комплексний підхід спрямований на максимальне зменшення ризиків та надання найвищого рівня захисту для криптовалютних активів в умовах постійно зростаючих викликів у кіберпросторі.

2. Розробка Сучасних Стратегій Захисту

У світлі постійного зростання кількості та складності кіберзагроз, розробка та реалізація ефективних стратегій захисту стає критично важливою умовою для стійкого та безпечного розвитку ринку криптовалютних активів. Цей процес передбачає впровадження технічних та соціальних підходів для максимальної ефективності заходів безпеки.

Технічні заходи націлені на використання передових технологій для захисту криптовалютних активів від різноманітних кіберзагроз. Шифрування, наприклад, використовується для захисту конфіденційності даних, забезпечуючи їхнє перетинання та непроникність для несанкціонованих осіб. Системи виявлення вторгнень дозволяють вчасно виявляти та реагувати на потенційно шкідливі дії, зменшуючи можливість завдання значних збитків.

Соціальні стратегії включають в себе комплекс заходів, спрямованих на удосконалення кібергігієни користувачів. Це охоплює навчання їх правилам безпеки, своєчасне оновлення програмного забезпечення, усвідомлення ризиків та відповідального використання криптовалютних активів. Ініціативи для підвищення кіберосвідомості гравців на ринку, включаючи як індивідуальних інвесторів, так і корпорації, стають необхідним елементом загального стратегічного плану безпеки.

Інтеграція технічних та соціальних аспектів в одну збалансовану стратегію захисту є ключем до створення комплексного та стійкого захисту. Технічні заходи надають захист від сучасних кіберзагроз, тоді як соціальні стратегії зменшують вразливість людського фактору та сприяють створенню культури безпеки в середовищі використання криптовалют.

Постійне вдосконалення та адаптація стратегій є невід'ємною частиною їх ефективності. Сучасні кіберзагрози розвиваються, тому необхідно постійно вдосконалювати заходи безпеки, враховуючи нові технології та методи атак.

Такий інтегрований підхід до розробки стратегій захисту є важливою складовою сталого та успішного розвитку ринку криптовалютних активів.

3. Виклики та Можливості Ринку

В умовах постійної еволюції кіберзагроз ринок криптовалютних активів стикається з рядом значущих викликів, які можуть значно вплинути на його стабільність та безпеку. Одночасно ці виклики створюють інноваційні можливості для вдосконалення стратегій захисту та забезпечення сталого розвитку цього динамічного ринку.

Зростання кількості кіберзагроз є основним викликом для ринку криптовалютних активів. Зловмисники постійно розвивають свої методи, використовуючи нові технології та тактики для отримання несанкціонованого доступу до цифрових активів. Підвищення рівня ускладненості атак вимагає постійного вдосконалення технічних та соціальних стратегій захисту.

Неодноразові інциденти кібербезпеки на ринку криптовалют, такі як атаки на обмінні платформи та криптогаманці, підкреслюють необхідність ефективних заходів захисту. Великі втрати, спричинені такими інцидентами, можуть вплинути на довіру інвесторів та загрожувати сталому розвитку ринку.

Швидкі зміни в регуляторному середовищі є ще одним важливим викликом для ринку криптовалютних активів. Відсутність чітких та стабільних нормативів може призвести до правової невизначеності, що ускладнює впровадження ефективних заходів безпеки та може призвести до ризиків для учасників ринку.

Можливості для інновацій та розвитку виникають з необхідності вирішення вищезазначених викликів. Розробка та впровадження нових технологій, таких як розширені методи шифрування, аналіз поведінки, та використання штучного інтелекту для виявлення загроз, можуть покращити ефективність заходів безпеки.

Постійне вивчення перспектив розвитку дозволяє адаптувати стратегії захисту до нових реалій. Технічний та соціальний аналіз тенденцій у кібербезпеці дозволяє оперативно відповідати на змінюючіся умови та запобігати майбутнім загрозам.

Усвідомлення та ефективне вирішення цих викликів стають ключовими факторами для забезпечення стійкого розвитку ринку криптовалютних активів та збереження довіри його учасників.

Можливості для інновацій та розвитку в кібербезпеці ринку криптовалют:

1) Розширення технічних засобів захисту: Інновації в області технічних засобів захисту, таких як блокчейн-технології для підвищення імунітету

криптогаманців або розробка безпечних протоколів обміну, можуть збільшити стійкість ринку до кіберзагроз.

2) Використання штучного інтелекту та машинного навчання: Розвиток алгоритмів штучного інтелекту для виявлення аномального поведінки та аналізу великих обсягів даних дозволить ефективно виявляти та запобігати кібератакам.

3) Співпраця та обмін інформацією: Створення механізмів для активної співпраці між учасниками ринку, обміну даними та інформацією про кіберзагрози, може стати ефективним методом для попередження широкого спектру атак.

4) Забезпечення відповідності до регуляторних стандартів: Розробка стандартів та визначень для кібербезпеки в сфері криптовалют може стати керівною зіркою для розробників стратегій захисту та сприяти створенню більш однорідного та безпечного середовища.

5) Кіберосвіта та навчання: Ініціативи з підвищення рівня кіберосвіти серед користувачів криптовалют можуть зменшити ризик людського фактору у кібербезпеці та сприяти створенню свідомого та відповідального споживача цифрових активів.

Враховуючи ці виклики та можливості, учасники ринку повинні постійно удосконалювати свої стратегії захисту та застосовувати інноваційні підходи для забезпечення стійкості та безпеки в умовах зростаючих кіберзагроз. Ретельне вивчення динаміки кіберпростору та активна реакція на зміни допоможуть створити розвинуту систему кібербезпеки, яка адаптується до нових викликів та забезпечує стійкий розвиток ринку криптовалютних активів.

5. Роль регуляторів та міжнародного співробітництва

Стабільність та довіра на криптовалютному ринку визначаються не лише технічними аспектами, але й регуляторним середовищем, що розвивається. Роль регуляторів у різних країнах стає ключовою для забезпечення ефективної охорони криптовалютних активів. У цьому

контексті, розробка та уніфікація міжнародних стандартів безпеки стає стратегічно важливою, оскільки вона дозволяє створити єдину базу для захисту криптовалютних активів на світовому рівні.

Регуляційна роль: Регулятори в різних країнах відіграють ключову роль у визначенні законодавчого середовища для криптовалют. Вони забезпечують впровадження стандартів безпеки та визначають правила для учасників ринку, з метою забезпечення надійності операцій та захисту користувачів.

Уніфікація стандартів: Розвиток та уніфікація міжнародних стандартів безпеки стає необхідністю в умовах глобалізації криптовалютних ринків. Це включає в себе розробку стандартів для технічних заходів безпеки, впровадження процедур ідентифікації та аутентифікації, а також визначення вимог до звітності та аудиту безпеки.

Міжнародне співробітництво: Забезпечення безпеки глобального криптовалютного ринку стає ефективнішим завдяки міжнародному співробітництву. Обмін інформацією про кіберзагрози та найкращими практиками в галузі кібербезпеки між регуляторами з різних країн дозволяє ефективно виявляти та протидіяти новим видам атак.

Поширення найкращих практик: Створення механізмів обміну найкращими практиками в галузі кібербезпеки стає критичним елементом. Це дозволяє регуляторам та учасникам ринку вчитися на помилках інших та швидше реагувати на нові загрози.

Прозорість та довіра: Роль регуляторів полягає не лише в утворенні правових рамок, але й в забезпеченні прозорості та довіри на ринку. Регуляторні стандарти повинні визначати процедури звітності та дотримання норм безпеки, що сприяє високому рівню довіри від учасників ринку та інвесторів.

Захист користувачів: Регулятори грають ключову роль у захисті прав та інтересів користувачів криптовалют. Вони встановлюють стандарти безпеки для обслуговування користувачів, включаючи засоби аутентифікації та захист особистих даних.

Врегулювання інновацій: Регулятори повинні бути готові врегулювати нові технології та інновації в галузі криптовалют. Забезпечення адаптивності правового середовища є важливим для того, щоб сприяти розвитку новаторських підходів до кібербезпеки.

Міжнародне регулювання: Оскільки криптовалютні ринки не мають чітко визначеної території, міжнародне регулювання є важливим елементом. Створення спільних норм та правил дозволяє уникнути вакууму в регулюванні та створює єдиний стандарт безпеки для глобального ринку.

Сприяння інноваціям: Здорове регулювання створює екосистему, в якій інновації можуть розвиватися. Регулятори повинні сприяти та заохочувати технологічний прогрес, забезпечуючи при цьому його безпеку та стійкість.

Міжнародне співробітництво та уніфікація стандартів безпеки створюють основу для сталого та надійного розвитку глобального криптовалютного ринку, забезпечуючи високий рівень захисту для всіх його учасників.

В цілому, взаємодія регуляторів та міжнародне співробітництво грають важливу роль у створенні безпечного, стабільного та надійного середовища для розвитку криптовалютних активів. Регулювання, яке враховує технологічний характер криптовалют та активно сприяє їхньому захисту, стає фундаментальним елементом довгострокового успіху цього ринку.

6. Соціоекономічні впливи

Посилення заходів безпеки на ринку криптовалют створює значущий вплив на його соціоекономічну динаміку, охоплюючи різні аспекти, від довіри інвесторів до ставлення регуляторів.

Довіра інвесторів: Заходи безпеки прямо впливають на довіру інвесторів до криптовалютних активів. Захищеність від кіберзагроз та кращі практики забезпечення можуть сприяти збільшенню довіри інвесторів до цього ринку, стимулюючи їхню активність та залучення нових учасників.

Легітимність торгових платформ: Заходи безпеки сприяють формуванню легітимності криптовалютних торгових платформ. Якщо

платформа виявляє високий рівень безпеки, це стає ключовим фактором для інвесторів, роблячи ринок більш привабливим і серйозним.

Ставлення регуляторів: Захист криптовалютних активів визначає ставлення регуляторів до цього виду активів. Якщо відбувається посилення заходів безпеки, це може сприяти створенню позитивного регуляторного середовища, що, в свою чергу, сприятиме сталому розвитку ринку.

Взаємодія бізнес-середовища та фінансового сектору: Захист криптовалютних активів може змінити взаємодію між бізнес-середовищем та фінансовим сектором. Якщо криптовалюти стають більш безпечними та стабільними, це може привести до більш глибокої інтеграції цих активів у фінансову систему та бізнес-процеси.

Економічні наслідки: Загальні економічні наслідки включають зростання обсягів інвестицій у криптовалютні активи, розвиток нових фінансових інструментів та збільшення капіталізації ринку. Вдосконалення заходів безпеки може визначати темпи розвитку цього сектору та його внесок у глобальну економіку.

В цілому, ефективні заходи безпеки відіграють ключову роль у формуванні стійкого, довіреного та привабливого для інвесторів криптовалютного ринку, впливаючи на різноманітні соціоекономічні виміри його функціонування.

У світлі стрімкого розвитку ринку криптовалютних активів, безпека стає критичною складовою для його успішного та сталого розвитку. Кібербезпека визначає не лише захист від потенційних загроз, але й впливає на довіру учасників ринку, приваблює нових інвесторів та визначає ступінь стабільності цього сектору.

Розробка та впровадження ефективних стратегій захисту, які ураховують як технічні, так і соціальні аспекти, стає визначальним фактором для формування майбутнього ринку криптовалютних активів. Технічні інновації, такі як блокчейн, та заходи безпеки на рівні користувача взаємодіють, створюючи синергію для стійкого та безпечного розвитку ринку.

Регулятори та міжнародна співпраця визначають ефективність системи захисту. Спільні стандарти безпеки та обмін досвідом стають фундаментом для глобальної стійкості криптовалютного ринку. Також, регулювання повинно бути адаптивним до технологічних інновацій, щоб сприяти їхньому розвитку та впровадженню в галузі.

Узагальнюючи, кібербезпека є визначальним чинником для стабільності та перспектив ринку криптовалютних активів у довгостроковій перспективі. Заходи безпеки, що об'єднують технічні та соціальні аспекти, разом із здоровим регулюванням і технологічними інноваціями, будуть сприяти створенню надійного та привабливого середовища для розвитку цього важливого сегменту фінансового ринку.

ВИСНОВКИ

Магістерська робота є комплексним дослідженням, спрямованим на розробку та моделювання стратегії захисту криптовалютних активів. У роботі були розглянуті та проаналізовані ключові аспекти, що визначають безпеку цих активів, включаючи технологічні, ринкові та соціально-психологічні аспекти.

У розділі 1 роботи було детально досліджено технологію блокчейн, яка є основою для функціонування криптовалют, а також проаналізовано проблеми та перспективи розвитку ринку криптовалютних активів. Визначено концептуальні засади моделювання стратегії захисту криптовалют, які враховують специфіку цих активів.

У другому розділі вивчено технологічні аспекти захисту, ринкові та соціально-психологічні методи захисту криптовалютних активів, а також розглянуто методи прогнозування ризиків на ринку. Цей розділ сприяв розумінню комплексності взаємодії різних аспектів захисту.

Розділ 3, присвячений стратегії захисту гаманців, включає оцінку ефективності існуючих стратегій, розробку оптимізаційної (імітаційної) моделі та розгляд перспектив розвитку ринку криптовалют з урахуванням розроблених стратегій захисту.

У висновках можна підкреслити, що розвиток ринку криптовалют потребує не лише новаторських підходів у використанні технологій блокчейн, але й ефективних стратегій захисту. Отримані результати свідчать про те, що комплексний підхід, який об'єднує технічні та соціальні аспекти захисту, може забезпечити стійкість та безпеку криптовалютних активів у змінному середовищі.

Дана магістерська робота може слугувати підґрунтям для подальших досліджень у сфері кібербезпеки криптовалютних ринків та розробки нових стратегій захисту. Завдяки врахуванню різних аспектів, вона може бути використана як орієнтир для розробників політики безпеки, а також для

компаній та індивідуальних користувачів, які працюють з криптовалютними активами.

В контексті швидкого розвитку технологій та поширення криптовалют як альтернативних фінансових інструментів, важливість забезпечення найвищого рівня безпеки для користувачів і їхніх криптовалютних активів надто важлива. Розглядаючи результати досліджень, можна виділити кілька перспектив та висновків, які визначать майбутній розвиток ринку криптовалют:

1. Досягнення максимальної ефективності в захисті криптовалют вимагає інтеграції технічних заходів з соціальними стратегіями. Оптимальне поєднання технічних аспектів (шифрування, систем виявлення вторгнень) і соціальних методів (освіта користувачів, підвищення кібергігієни) сприятиме створенню найбільш надійної системи захисту.

2. Використання імітаційних моделей, як розглядається в розділі 3, може слугувати ефективним інструментом для оптимізації стратегій захисту. Моделювання різних сценаріїв дозволяє оцінити ефективність стратегій у віртуальному середовищі перед їхнім впровадженням в реальному житті.

3. Розробка та уніфікація стандартів безпеки на міжнародному рівні стане ключовим чинником для створення стабільного криптовалютного ринку. Регулятори мають активну роль у формуванні норм та правил, які забезпечать безпеку та довіру учасників ринку.

4. Розвиток нових технологій, таких як розширені блокчейн-рішення, та їхня адаптація в системах криптовалют створюють нові можливості, але й виклики для безпеки. Інновації в галузі захисту повинні швидко адаптуватися до змін технологічного ландшафту.

5. Посилення заходів безпеки може впливати на соціоекономічні аспекти ринку криптовалют. Довіра інвесторів, легітимність торгових платформ та реакція регуляторів - всі ці фактори важливі для довгострокового стабільного розвитку ринку.

У цілому, враховуючи зазначені перспективи, важливо продовжувати наукові та практичні дослідження в області кібербезпеки криптовалют. Це допоможе створити розвинуті та ефективні стратегії захисту, що відповідають найновішим викликам і можливостям цього унікального ринку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Біткоїн – прогноз на 2023, 2025 та 2030 рр. URL: https://tradersunion.com/ru/currencies/forecast/btc-usd.

2. Біткоїн Україна : Майданчик для спілкування та інформаційний центр щодо використання технологій блокчейн (біткоїн) та інших відкритих розподільчих протоколів в Україні. URL: http://www.bitcoinua.org/theboard/

3. Взлети та падіння біткоїну, The Economist. Buttonwood's. Tales from the crypto. URL: https://www.economist.com/blogs/buttonwood/2018/01/tales-crypto-1

4. Галушка Є. О. Сутність криптовалют та перспективи їх розвитку. Молодий вчений. 2017. № 4. С. 634–638.

5. Гармідер Л. Д., Орлова А. В. Особливості розвитку вітчизняної електронної комерції. Європейський вектор економічного розвитку. Економічні науки. 2015. № 1. С. 58–65.

6. Гусєва І. І., Петрова Т. О. Тенденції розвитку криптовалют на ринку України. Науковий вісник Між- народного гуманітарного університету. Серія : Економіка і менеджмент. 2017. Вип. 24(1). С. 48–50. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_ S21STR=Nvmgu_eim_2017_24(1) 12.

7. Давидова І. Технологія блокчейн: перспектива розвитку в Україні. Часопис цивілістики. 2017. №. 26. С. 38–41.

8. Домінова І. В. Ризик шахрайства в умовах функціонування електронного банкінгу. Науково-виробничий журнал «Бізнеснавігатор». 2017. № 4-2. С. 92–98.

9. Дубенський В. С. Еволюція Bitcoin. Чому валюти боїться влади? URL: http://chp.com.ua/all-news/item/37954-evolyutsiyabitcoinpochemu-valyutyi-boitsyavlast.

10. Жидовська Н. М. Передумови запровадження оподаткування операцій із криптовалютами в Україні. Вісник Одеського національного університету ім. І. І. Мечникова, 2019. Т. 24. Вип. 2 (75). С. 108–112.

11. Закон України «Про віртуальні активи» від 17.02.2022 року №2074 – IX. URL:https://zakon.rada.gov.ua/laws/show/2074-20#Text

12. Закон України «Про Національний банк України» № 679-14. URL: http://zakon3.rada.gov.ua/laws/show/679-14

13. Інтерв'ю Матоніса Дж. Bussiness Insider. URL: https://www.rbc.ru/crypto/news/5ac236a39a794767b75da9ef

14. Карчева Г., Лернатович Р., Кавецький В. Використання технології «блокчейн» як фактор підвищення ефективності фінансової сфери. Банківська справа. 2017. № 2

15. Ковальчук Т., Паливода К. Цифрова валюта як віртуальне джерело фіктивного капіталу. Банківська справа. 2014. № 1-2

16. Колдовський А. В., Чернега К. В. Проблемні аспекти теоретичного осмислення криптовалюти як явища сучасної інформаційної економіки. Проблеми і перспективи розвитку банківської системи України. 2015. № 42.

17. Король М.М., Дір І.Ю., Вароді В.М. Особливості обігу криптовалюти як тенденція цифровізації глобальних фінансів. Науковий вісник Ужгородського національного університету. 2019. № 28(1). С. 170–173.

18. Костюченко В. М., Малиновська А. М., Мамонова А. В. Облік криптовалют за міжнародними стандартами. Modern Economics. 2020. № 21(2020). С. 122–128. URL: https://modecon.mnau.edu.ua/ issue/21-2020/kostyuchenko.pdf.

19. Криптовалюта в Україні: все, що треба знати. URL: http://nk.org.ua/ekonomika/kriptovalyuta-v-ukrayini-vse-schotreba-znati- 116647

20. Кувшинова А. Криптовалюта: гроші чи мильна бульбашка? Бухгалтерський облік і аудит. 2018. № 1. С. 29–38.

21. Кунета М. Думка: чому протокол біткоїна не зупинити. URL: https://whattonews.ru/reviews/13939

22. Лук’янчук Р. В. Сучасні виклики, пов’язані із розвитком криптоіндустрії. Інформація і право. № 1(40)/2022. С. 72–81. URL: http://ippi.org.ua/sites/ default/files/9_23.pdf.

23. Мельниченко О. В. Теорія, методологія та практика обліку, аналізу і аудиту електронних грошей в банках. Житомир: ЖДТУ, 2015. 384 с.

а. Міністерство та комітет інформаційних технологій URL: https://thedigital.gov.ua/news/ukraina-legalizuvala-kriptosektor-prezident-pidpisav-profilniy-zakon

24. Молчанова Е., Солодковський Ю. Глобальна сервісна природа сучасних криптовалют. Міжнародна економічна політика. 2014. № 1.

25. Назаров Є. М. Особливості криптовалют та способи їх добування. Українські студії в європейському контексті: зб. наук. пр. 2022. № 5. С. 196–200.

26. Одарченко А. М., Сподар К. В. Особливості електронної комерції та перспективи її розвитку в Україні. Бізнес Інформ. 2015. № 1. С. 342–346.

27. Оліярник М. Криптовалюта в Україні. Все, що треба знати. URL: http://nv.ua/techno/it-industry/kriptovaljuta-bitcoinv-ukraine-vse-chto-nuzhno-znat-1918518.htm

28. Офіційний сайт Міністерства фінансів України. URL: https://minfin.com.ua

29. Петрук О. М., Новак О. С. Сутність криптовалюти як методологічна передумова її облікового відображення. Вісник Житомирського державного технологічного університету. Серія : Економічні науки. 2017. No 4 (82). С. 48–55.

30. Поливка Н. Криптовалюти і «різноманітні біткоіни» URL: http://yurgazeta.com/publications/practice/informaciyne-pravo- telekomunikaciyi/ kriptovalyuti-i-riznomanitni-bitkoini.html

31. Поплавський О. О. Криптавалюта як об’єкт економічного аналізу в страхових компаніях. Вісник ЖДТУ. 2016. № 4.

32. Принцип роботи блокчейну. URL: https://cryptonisation.ru/chto-takoye- blokcheyn-prostymi-slovami/

33. Рейтинг бірж. URL: https://coinmarketcap.com/rankings/exchanges/

34. Самоходський І., Шелест О. Зелена книга регулювання ринку криптовалют. Київ, 2018. URL:: https://regulation.gov.ua/book/91-zelena-kniga-regu- luvannarinku-kriptovalut.

35. Сидор Г. В. Криптовалюта – гроші майбутнього / Андрусів, Г. В. Сидор, Г. І. Давидовська // Актуальні проблеми економіки та управління в епоху глобальних викликів і загроз : зб. матер. Всеукр. наук.-практ. конф., (м. Дніпро, 26–27 квіт. 2018 р.). – в 2-х томах. – Т. 2. – Дніпро, 2018. – С. 304– 306.

36. Спільник І., Ярощук О. Інституалізація криптовалюти: регулювання, правовий статус, облік і оподаткування. Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації. 2020. Випуск 2. С. 81–92. URL: https://journals.indexcopernicus.com/ api/file/viewByFileId/1079546.pdf.

37. Тапскотт А., Тапскотт Д. Технологія блокчейн. URL: http://tornado.org.ru/details.php?id=32893.

38. Ширінян Л. В., Роганова Г. О., Ширінян А. С. Вплив факторів на формування вартості біткойна. Проблеми економіки. 2018. № 2 (36). С. 450–458. URL: https://www.problecon.com/export_pdf/problems-of-economy-2018-2_0-pages-450_458.pdf.

39. Штепенко К.П., Миргородська А.О. Стан і перспективи розвитку криптовалюти у світі. URL: https://fp.cibs.ubs.edu.ua/files/1802/18sk_kvs.pdf

40. Яцик Т. В. Методика фінансового обліку криптовалюти як особливого виду електронних грошей. Молодий вчений. 2017. № 2 (42). С. 349–354.

41. Andreas M. Antonopoulos, Mastering Bitcoin. – URL: https://github.com/bitcoinbook/bitcoinbook

42. Binance. URL: https://www.binance.com/uk-UA/trade/BTC_BUSD?theme=dark&type=spot

43. Investfunds. URL: https://investfunds.ru.

44. Jim Brikman, Bitcoin by Analogy URL: http://brikis98.blogspot.com/2014/04/bitcoin-by-analogy.html.

45. Kashchena N., Kovalevska N., Nesterenko I. Organizational and methodological aspects of audit of integrated reporting of enterprise. Zeszyty naukowe wyższej szkoły technicznej w katowicach. Wyższej Szkoły Technicznej w Katowicach. 2021. NR 14. s. 153-164. URL: http://www.wydawnictwo.wst.pl/uploads/files/b0476ba555ccaead5a41dfab07ee2f39.pdf

46. Ponsford, M. A Comparative Analysis of Bitcoin and Other Decentralised Virtual Currencies: Legal Regulation in the People's Republic of China, Canada, and the United States. Hong Kong Journal of Legal Studies. 2015. Vol. 9. URL: http://ssrn.com/ abstract=2554186

47. Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry/Polasik Michal, Piotrowska Anna, Wisniewski Tomasz Piotr, Kotkowski Radosław, Lightfoot Geoff. URL: http://ssrn.com/ abstract=2516754

48. Saifedean Ammous, The Bitcoin Standard. URL: http://www.altcoincalendar.info/r/article/h72. – 28.04.201

49. The 2022 Global Crypto Adoption Index. URL: https://blog.chainalysis.com/reports/2022-global- crypto-adoption-index/#top-20

50. TradingView. Ринок криптовалют. URL: https://www.tradingview.com/markets/cryptocurrencies/prices-all