**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ДОПУСТИТИ ДО ЗАХИСТУ:**
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025 р.

# ПОЯСНЮВАЛЬНА ЗАПИСКА

## кваліфікаційної роботи

**галузь знань** 12 Інформаційні технології
(шифр і назва галузі знань)
**спеціальність** 125 Кібербезпека
(код і назва спеціальності)
**освітній ступень** бакалавр
**освітня програма** Кібербезпека
(назва освітньо-професійної програми)
**на тему:** «Механізм захисту криптовалютних бірж та холодних гаманців»

**Виконавець:** студентка IV курсу, групи КБ-43

_____ **Яна БОНДАРЕНКО**
(підпис) (ім'я, прізвище)

| | **Підпис** | **Ім'я ПРІЗВИЩЕ** |
|---|---|---|
| **Керівник** | | Яніна ШЕСТАК |
| **Нормоконтроль** | | Іван БІЛОКОНЬ |

**Київ 2025**

**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО:**
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«29» листопада 2024 р.

# ЗАВДАННЯ
## на виконання кваліфікаційної роботи

**спеціальності** 125 Кібербезпека
(код і назва спеціальності)

**освітньої програми** Кібербезпека
(назва освітньо-професійної програми)

**Студентці** **КБ-43** **Бондаренко Яні Віталіївні**
(група) (прізвище ім'я по батькові)

**Тема кваліфікаційної роботи** Механізм захисту криптовалютних бірж та холодних гаманців

### 1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

### 2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Методи захисту криптовалютних бірж та холодних гаманців від кібератак та несанкціонованого доступу.

### 3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

У межах дослідження проведено аналіз актуальних методів захисту криптовалютних бірж та холодних гаманців, на основі отриманих даних сформовано концепцію комплексної моделі захисту, що охоплює технічні, організаційні та криптографічні заходи. Було розроблено інструмент CryptoColdShare для безпечного розподіленого зберігання seed-фраз.

### 4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

**Практична цінність** Розробка інструменту CryptoColdShare та формування

комплексної моделі захисту

**5. ДАТА ВИДАЧІ ЗАВДАННЯ**

Дата видачі завдання: 29 листопада 2024 року

Завдання видала _____ (підпис) Яніна ШЕСТАК (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Яна БОНДАРЕНКО (ім'я, прізвище)

**КАЛЕНДАРНИЙ ПЛАН**

| № п/п | Найменування етапів робіт | Строки виконання робіт (початок-кінець) | Відмітка про виконання |
|---|---|---|---|
| 1 | Уточнення постановки задачі | 29.11.2024 – 22.01.2025 | *виконано* |
| 2 | Аналіз літератури | 29.01.2025 – 15.02.2025 | *виконано* |
| 3 | Обґрунтування вибору рішення | 16.02.2025 – 25.02.2025 | *виконано* |
| 4 | Вивчення сучасних загроз і підходів до захисту криптовалютних платформ | 16.02.2025 – 04.03.2025 | *виконано* |
| 5 | Дослідження особливостей роботи холодних гаманців та типових вразливостей | 05.03.2025 – 21.03.2025 | *виконано* |
| 6 | Узагальнення проблем і розробка інструменту CryptoColdShare | 22.03.2025 – 08.04.2025 | *виконано* |
| 7 | Формування комплексної моделі захисту біржі та холодних гаманців | 09.04.2025 – 10.05.2025 | *виконано* |
| 8 | Оформлення пояснювальної записки | 11.05.2025 – 27.05.2025 | *виконано* |
| 9 | Підготовка до захисту кваліфікаційної роботи | 28.05.2025 – 13.06.2025 | *виконано* |

Завдання видала _____ (підпис) Яніна ШЕСТАК (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Яна БОНДАРЕНКО (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

# РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 70 сторінок основного тексту, 2 таблиці та 9 рисунків. Список використаних джерел містить 25 найменувань і займає 3 сторінки.

*Метою роботи* є аналіз сучасних загроз у сфері криптовалют, вивчення існуючих методів захисту криптовалютних бірж і холодних гаманців та розробка ефективного плану безпеки з впровадженням інноваційного інструменту для зниження кіберризиків.

Для досягнення зазначеної мети поставлено наступні завдання:

1. Проаналізувати сучасний стан безпеки криптовалютних бірж та холодних гаманців, а також основні види кіберзагроз, які їм загрожують.
2. Дослідити існуючі методи та технології захисту, які використовуються на криптовалютних платформах і в холодних гаманцях.
3. Розробити інтегровану стратегію захисту криптовалютних бірж та холодних гаманців.
4. Розробити та реалізувати програмний інструмент CryptoColdShare для безпечного розподіленого зберігання seed-фраз.
5. Оцінити рівень безпеки, автономності та практичної придатності запропонованого рішення у контексті cold storage для криптовалют.

*Об'єктом дослідження* є процес забезпечення безпеки криптовалютних бірж та холодних гаманців у контексті сучасних кіберзагроз.

*Предметом дослідження* є методи, технології та інструменти, що використовуються для забезпечення безпеки криптовалютних бірж і холодних гаманців, а також шляхи їх удосконалення.

Методи дослідження:

- аналіз наукових джерел, нормативних документів та відкритих публікацій;

- компаративний аналіз типів криптогаманців і біржових платформ;
- аналіз загроз та типових вразливостей;
- функціональне тестування працездатності системи відновлення seed-фраз.

*Практичною цінністю* є створення інструменту CryptoColdShare для безпечного розподіленого зберігання seed-фраз, який може бути використаний як самостійне рішення або як компонент комплексної системи захисту криптовалютних активів.

*Актуальність роботи* полягає в зростаючій кількості кіберзагроз, спрямованих на криптовалютні біржі та гаманці, що вимагає впровадження нових підходів до захисту цифрових активів, зокрема розробки безпечних та автономних рішень для зберігання seed-фраз та управління доступом до криптовалют.

*Ключові слова:* криптовалюта, холодний гаманець, гарячий гаманець, криптовалютна біржа, кібербезпека, захист даних, приватний ключ, seed-фраза, Shamir Secret Sharing, безпечне зберігання, розподілені системи, інформаційна безпека.

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

| | | |
|---|---|---|
| CEX | – | Centralized Exchange |
| DEX | – | Decentralized Exchange |
| KYC | – | Know Your Customer |
| USDT | – | Tether (Stablecoin) |
| Dapps | – | Decentralized Applications |
| DeFi | – | Decentralized Finance |
| DDoS | – | Distributed Denial of Service |
| NFT | – | Non-Fungible Token |
| DAO | – | Decentralized Autonomous Organization |
| 2FA | – | Two-Factor Authentication |
| AML | – | Anti-Money Laundering |
| SSO | – | Single Sign-On |
| HTTPS | – | HyperText Transfer Protocol Secure |
| API | – | Application Programming Interface |
| MITM | – | Man-in-the-Middle Attack |
| SSL/TLS | – | Secure Sockets Layer / Transport Layer Security |
| XSS | – | Cross-Site Scripting |
| SQL | – | Structured Query Language |
| CSRF | – | Cross-Site Request Forgery |
| RBAC | – | Role-Based Access Control |
| ABAC | – | Attribute-Based Access Control |
| PBAC | – | Policy-Based Access Control |
| TBAC | – | Time-Based Access Control |

# ЗМІСТ

# ВСТУП

Безпека криптовалютних бірж та холодних гаманців є важливим аспектом у сучасній цифровій економіці. Зростання популярності криптовалютних активів супроводжується збільшенням кіберзагроз, спрямованих на викрадення коштів та компрометацію особистих даних користувачів. Вразливість криптовалютних бірж, що часто стають об’єктами хакерських атак, створює загрозу не лише для окремих користувачів, але й для всієї фінансової системи, яка поступово інтегрує криптовалютні технології. Вивчення питань безпеки та розробка ефективних планів захисту є критично важливими для мінімізації ризиків і забезпечення довіри до криптовалют як фінансового інструменту.

Окрім криптовалютних бірж, увагу варто приділити холодним гаманцям, які забезпечують високий рівень безпеки завдяки зберіганню активів офлайн. Проте, навіть ці засоби захисту можуть бути вразливими у випадках фізичного доступу до пристроїв чи їх неналежного використання. Розробка комплексних стратегій безпеки, які включають як технічні, так і організаційні заходи, допоможе мінімізувати загрози, зберігаючи приватність користувачів та їхні активи. Це особливо важливо в умовах постійного вдосконалення методів атак та зростання кіберзлочинності.

Дослідження теми безпеки криптовалютних бірж та холодних гаманців дозволяє не лише аналізувати існуючі загрози, але й пропонувати інноваційні підходи до їх попередження. Розробка планів захисту, адаптованих до сучасних реалій, сприятиме розвитку ринку криптовалют та підвищенню рівня захищеності користувачів. Врахування технологічних трендів, таких як блокчейн-автентифікація чи інтеграція штучного інтелекту, відкриває нові можливості для вдосконалення безпекових систем. Таким чином, дослідження цієї теми є важливим не лише з практичної, але й з наукової точки зору.

# РОЗДІЛ 1
# АНАЛІЗ ЗАГРОЗ У СФЕРІ КРИПТОВАЛЮТНИХ БІРЖ ТА ГАМАНЦІВ

## 1.1 Загальна характеристика криптовалютних бірж та гаманців

Криптовалюта - це цифрові активи, вартість яких визначається попитом і пропозицією користувачів, а не державними фінансовими регуляторами чи курсами національних валют. Вона є інтернаціональною та не прив’язана до жодної країни, оскільки не має централізованого емітента чи контролюючого органу. Завдяки блокчейн-технології транзакції з криптовалютою децентралізовані, що забезпечує незалежність від банківської системи та високу прозорість фінансових операцій.

Попри свої переваги, криптовалюта залишається частково конвертованою, а її використання може обмежуватися залежно від законодавства конкретної країни. Деякі держави активно підтримують та регулюють криптовалютний ринок, дозволяючи громадянам здійснювати розрахунки та інвестувати в цифрові активи, тоді як інші обмежують або навіть забороняють такі операції. Рівень довіри до криптовалюти з боку фінансових установ визначає її інтеграцію в офіційні економічні процеси та можливість використання в повсякденному житті.

Криптовалютні біржі - це онлайн-платформи, які дозволяють користувачам купувати, продавати, обмінювати та торгувати криптовалютами. Вони виконують функцію посередника між покупцями та продавцями, надаючи інструменти для здійснення угод, аналітики ринку та управління цифровими активами [1]. Біржі можуть мати різні рівні доступу, вимоги до верифікації та безпеки, що впливає на їхню зручність та популярність серед користувачів. Криптовалютні біржі поділяються на два основних типи: централізовані (CEX) та децентралізовані (DEX). Централізовані біржі управляються компанією або організацією, яка контролює всі операції та зберігає кошти користувачів. Вони

забезпечують високу ліквідність, швидкість транзакцій та широкий вибір торгових пар, але вимагають проходження верифікації (KYC). Прикладами CEX є Binance, Coinbase, Kraken.

Децентралізовані біржі працюють без посередників завдяки смарт-контрактам на блокчейні. Вони дозволяють користувачам здійснювати торгівлю без реєстрації та контролю з боку централізованої структури, що підвищує анонімність і безпеку. Однак такі платформи можуть мати нижчу ліквідність, вищі комісії за транзакції та складніший інтерфейс. Прикладами DEX є Uniswap, PancakeSwap, SushiSwap.

Криптовалютні гаманці - це спеціальні програми або пристрої, які використовуються для зберігання, надсилання та отримання криптовалют. Вони працюють на основі криптографії та дозволяють користувачам управляти своїми цифровими активами за допомогою приватних і публічних ключів. Приватний ключ є унікальним кодом, який дає власнику доступ до криптовалютних коштів, тоді як публічний ключ використовується для отримання платежів. Безпека гаманця залежить від його типу та методів зберігання ключів.

Існує два основних типи криптовалютних гаманців: гарячі (hot wallets) та холодні (cold wallets). Гарячі гаманці підключені до інтернету, що робить їх зручними для щоденних транзакцій, але водночас вразливими до хакерських атак (наприклад, Trust Wallet, MetaMask, Exodus). Холодні гаманці зберігають приватні ключі в офлайн-середовищі, що забезпечує вищий рівень безпеки, але ускладнює доступ до коштів (приклади: Ledger, Trezor, паперові гаманці). Вибір гаманця залежить від потреб користувача: для активної торгівлі підходять гарячі гаманці, а для довгострокового зберігання - холодні [2].

Криптовалютні біржі та гаманці відіграють ключову роль у криптовалютній екосистемі, забезпечуючи інфраструктуру для доступу, управління та використання цифрових активів. Біржі слугують основними платформами для купівлі та продажу криптовалют, надаючи користувачам можливість конвертувати фіатні гроші в цифрові активи та навпаки. Вони також виконують функцію ліквідності, сприяючи формуванню справедливої ринкової

ціни завдяки механізму попиту та пропозиції. Гаманці, своєю чергою, забезпечують безпечне зберігання та управління криптовалютами, дозволяючи користувачам здійснювати транзакції без необхідності постійного звернення до бірж.

Однією з основних функцій криптобірж є купівля та продаж криптовалют. Користувачі можуть обирати різні торгові інструменти, включаючи спотову торгівлю, ф'ючерси та маржинальні операції. Завдяки біржам інвестори та трейдери можуть спекулювати на зміні курсу криптовалют, отримуючи прибуток від короткострокових чи довгострокових угод. Багато платформ також пропонують автоматизовані механізми торгівлі, такі як стоп-лоси та лімітні ордери, що дозволяють ефективно керувати ризиками.

Крім купівлі та продажу, біржі та гаманці виконують функцію обміну криптовалют. Вони дозволяють користувачам обмінювати одну криптовалюту на іншу, наприклад, Bitcoin на Ethereum чи USDT. Це особливо важливо для трейдерів і власників цифрових активів, які бажають диверсифікувати свій портфель або скористатися перевагами конкретних блокчейн-екосистем. Децентралізовані біржі (DEX) забезпечують обмін безпосередньо між користувачами через смарт-контракти, що усуває необхідність у посередниках та підвищує рівень децентралізації [3].

Ще одна важлива функція криптовалютних гаманців - зберігання та переказ активів. Гаманці дозволяють власникам криптовалюти безпечно зберігати приватні ключі, які дають доступ до коштів. Вони також забезпечують можливість швидкого переказу активів між користувачами по всьому світу без участі банківської системи. Це робить криптовалютні платежі зручним та ефективним засобом фінансових операцій, особливо для міжнародних переказів із мінімальними комісіями та без затримок.

Отже, підсумовуючи, криптовалютні біржі та гаманці є невід'ємною частиною криптовалютної екосистеми, забезпечуючи користувачам зручний доступ до цифрових активів. Біржі виконують роль посередника між покупцями та продавцями, забезпечуючи ліквідність ринку, а також надаючи інструменти

для торгівлі, обміну та аналізу ринку. Гаманці, у свою чергу, гарантують безпечне зберігання криптовалют, управління приватними ключами та здійснення швидких транзакцій.

## 1.2 Типи криптовалютних гаманців: гарячі та холодні

Гарячі гаманці - це цифрові гаманці, що мають постійне підключення до Інтернету, забезпечуючи швидкий доступ до криптовалют. Вони використовуються для зберігання, надсилання та отримання цифрових активів. Основна перевага таких гаманців - зручність і простота використання, що робить їх популярними серед трейдерів та користувачів, які часто здійснюють транзакції. Проте їхня підключеність до мережі робить їх вразливими до кібератак, тому для довгострокового зберігання значних сум краще використовувати холодні гаманці.

Одним із найпоширеніших гарячих гаманців є MetaMask. Це браузерне розширення та мобільний додаток, що дозволяє взаємодіяти з блокчейном Ethereum та іншими сумісними мережами. MetaMask підтримує зберігання та управління токенами ERC-20, а також дає змогу користувачам підключатися до децентралізованих додатків (DApps), таких як DeFi-платформи та NFT-маркети. Гаманець має функцію збереження приватних ключів локально на пристрої користувача, але залишається вразливим до фішингових атак і зломів браузерних розширень.

Ще одним популярним гарячим гаманцем є Trust Wallet - мобільний додаток для зберігання криптовалют, який підтримує тисячі різних токенів і блокчейнів. Він дозволяє користувачам купувати, обмінювати та зберігати криптовалюту безпосередньо зі смартфона. Trust Wallet також має вбудований браузер для доступу до децентралізованих додатків, що робить його зручним для роботи з DeFi-платформами. Завдяки децентралізованому підходу користувачі контролюють свої приватні ключі, але при цьому ризики збереження активів на пристрої, підключеному до Інтернету, залишаються.

Ще один приклад - Exodus, який доступний як настільний і мобільний додаток. Цей гаманець відзначається зручним інтерфейсом, підтримкою понад 100 криптовалют і вбудованим механізмом обміну активів. На відміну від біржових гаманців, Exodus надає користувачам повний контроль над приватними ключами. Однак, як і інші гарячі гаманці, він залишається вразливим до атак хакерів та шкідливого програмного забезпечення. Тому користувачам рекомендується використовувати додаткові заходи безпеки, такі як двофакторна автентифікація та резервне копіювання ключів.

Гарячі гаманці є найпоширенішим типом криптовалютних гаманців, оскільки вони зручні у використанні та швидкі в налаштуванні. Вони постійно підключені до Інтернету, що дозволяє користувачам легко отримувати доступ до своїх криптоактивів. Створення гарячого гаманця відбувається автоматично при реєстрації на криптобіржі, встановленні мобільного або настільного додатку для зберігання криптовалют. Через свою доступність ці гаманці найкраще підходять для щоденного використання, включаючи трейдинг та оплату товарів і послуг.

Головна перевага гарячих гаманців полягає в їхній зручності: вони дозволяють швидко здійснювати транзакції без необхідності складних налаштувань. Наприклад, біржові гаманці також є гарячими, оскільки забезпечують миттєвий доступ до засобів на платформі. Однак для підвищення безпеки великі біржі зберігають більшу частину коштів користувачів у холодних гаманцях, зменшуючи ризик втрати активів через хакерські атаки. Звичайні мобільні або веб-гарячі гаманці такої функції не мають, що робить їх більш вразливими до зломів [4].

Основний недолік гарячих гаманців - безпека. Оскільки вони підключені до мережі, вони є потенційною мішенню для хакерів і фішингових атак. Зберігання значних сум криптовалют у гарячому гаманці може бути ризикованим, тому рекомендується тримати там лише необхідну кількість для повсякденного використання. Довгострокові інвестиції варто зберігати у холодних гаманцях, які не мають постійного доступу до Інтернету та забезпечують вищий рівень безпеки.

Холодні гаманці - це криптовалютні гаманці, які не підключені до Інтернету, що забезпечує високий рівень безпеки для зберігання цифрових активів. Оскільки вони не мають доступу до мережі, вони не піддаються атакам хакерів або фішинговим загрозам, які можуть вплинути на гарячі гаманці. Холодні гаманці часто використовуються для довгострокового зберігання великих сум криптовалют, оскільки вони значно знижують ризик крадіжки. Їх можна використовувати для зберігання приватних ключів, доступ до яких можна отримати тільки фізично, що робить їх ідеальними для інвесторів, які не потребують постійного доступу до своїх активів.

Одним із найпоширеніших типів холодних гаманців є апаратні гаманці. Це фізичні пристрої, які зберігають приватні ключі в зашифрованому вигляді. Відомими прикладами апаратних гаманців є Ledger Nano S, Ledger Nano X та Trezor. Ці пристрої підключаються до комп'ютера або мобільного пристрою лише при необхідності, що дозволяє здійснювати транзакції з максимальною безпекою [5]. Дані на таких пристроях не можуть бути виведені без фізичного доступу до самого гаманця, що забезпечує високу ступінь захисту від зломів та вірусів.

Іншим типом холодних гаманців є паперові гаманці, які являють собою фізичні документи, на яких надруковано публічні та приватні ключі. Це може бути просто текст або QR-коди, які використовуються для доступу до криптовалюти. Паперові гаманці не підключені до Інтернету і можуть бути збережені в надійному місці, наприклад, у банківському сейфі. Проте, якщо папір буде втрачено або пошкоджено, доступ до криптовалютних активів буде втрачено без можливості відновлення.

Холодні гаманці є одним із найбільш безпечних способів зберігання криптовалют, оскільки не підключені до Інтернету [6]. Їхня головна перевага полягає в тому, що вони практично виключають можливість хакерських атак або несанкціонованого доступу до активів. Для того щоб здійснити транзакцію, користувач повинен підключити свій холодний гаманець до Інтернету, що робить цей процес більш захищеним, порівняно з гарячими гаманцями. Вони

ідеально підходять для зберігання великих сум криптовалют, які не потрібно витрачати на постійній основі. Апаратні гаманці є одним з найпоширеніших видів холодних гаманців. Вони використовують фізичні носії, такі як USB-накопичувачі, для зберігання приватних ключів, що робить їх майже недоступними для хакерів. Апаратні гаманці пропонують зручний спосіб зберігання криптовалют без ризику їх крадіжки через Інтернет. Щоб здійснити транзакцію, користувач підключає апаратний гаманець до комп'ютера або мобільного пристрою через спеціальне програмне забезпечення і підписує операцію своїм приватним ключем.

Паперові гаманці працюють схожим чином, однак замість фізичного носія дані про публічний і приватний ключі записуються на фізичному аркуші паперу. Це робить їх дуже надійними з точки зору безпеки, але також вимагає обережного зберігання, адже фізичне пошкодження чи втрата паперу призведе до втрати доступу до криптовалют. Щоб витратити монети з паперового гаманця, потрібно імпортувати приватний ключ у гарячий гаманець. Хоча холодні гаманці є дуже безпечними, їхня непрактичність для повсякденних операцій з криптовалютами може стати значним мінусом для користувачів, які часто проводять транзакції.

Отже, підсумовуючи, гарячі гаманці є зручними для щоденного використання криптовалют, оскільки вони підключені до Інтернету, що дозволяє легко здійснювати транзакції через мобільні пристрої або комп'ютери. Вони ідеальні для трейдерів, які часто здійснюють операції, або для користувачів, які використовують криптовалюти для покупок. Однак, через підключення до мережі, вони менш безпечні, що може бути ризикованим для зберігання великих сум.

Водночас холодні гаманці пропонують значно вищий рівень безпеки, оскільки не підключені до Інтернету, що захищає їх від хакерських атак. Це робить їх ідеальними для зберігання великих сум криптовалют, особливо на довгий термін. Однак, процес здійснення транзакцій з холодного гаманця є менш

зручним і практичним, що може бути недоліком для тих, хто часто торгує або проводить операції.

### 1.3 Особливості централізованих і децентралізованих бірж

Централізовані біржі (CEX), такі як Binance, є платформами для онлайн-торгівлі, які виступають посередниками між покупцями та продавцями криптовалют. Вони функціонують за принципом «книги замовлень», де учасники біржі можуть виставляти свої ордери на купівлю чи продаж активів, а система знаходить найкращу пару для угоди. Важливим аспектом таких бірж є те, що вони зберігають контроль над користувацькими коштами та обробляють всі транзакції, що надає користувачам додаткову зручність, але і підвищує ризики щодо безпеки та довіри. Централізовані біржі (CEX) мають кілька переваг, які роблять їх популярними серед трейдерів та інвесторів. Однією з основних переваг є високі обсяги торгів, що забезпечують високу ліквідність на ринку. Наприклад, Binance, одна з найбільших централізованих бірж, регулярно фіксує щоденні обсяги торгів на суму понад 30 мільярдів доларів. Це дозволяє трейдерам швидко здійснювати покупки та продажі активів, не зустрічаючи проблем з ціною чи виконанням ордерів.

Централізовані біржі також дозволяють легко конвертувати фіатні валюти в криптовалюту та навпаки. Вони підтримують широкий спектр фіатних криптовалют, що дозволяє користувачам купувати біткоїни чи інші цифрові активи за своїми національними валютами, такими як гривня, долар чи євро. Це робить процес входу на крипторинок простим і зручним для новачків, які не мають криптовалют, але хочуть почати інвестувати. Крім того, централізовані біржі часто пропонують додаткові можливості для більш досвідчених трейдерів, такі як маржинальна торгівля, торгівля крипто-деривативами, біржовий стейкінг та інші інструменти. Це дає користувачам більше варіантів для отримання прибутку та здійснення складних фінансових операцій. Серед переваг також зручність використання, адже біржі зазвичай мають інтуїтивно зрозумілі

інтерфейси, що полегшують процес торгівлі навіть для новачків у криптопросторі.

Однак є й певні недоліки централізованих бірж. Один з основних - сувора політика "Знай свого клієнта" (KYC), яка вимагає від користувачів надання особистої інформації та проходження верифікації. Це може бути незручним для тих, хто хоче зберігати конфіденційність своїх операцій. Також варто пам'ятати, що у CEX гаманці є кастодіальними, що означає, що біржа зберігає ваші приватні ключі. Тому користувачі не мають повного контролю над своїми коштами, а все залежить від безпеки платформи. Більше того, біржі можуть бути привабливими цілями для хакерів, що робить їх вразливими до кіберзлочинів.

Децентралізовані біржі (DEX), такі як PancakeSwap або Uniswap, на відміну від централізованих, не мають єдиного управлінця або організації, що контролює процеси на біржі. Вони базуються на смарт-контрактах - спеціальних алгоритмах, які автоматично виконують умови угоди без необхідності посередників. Це дозволяє трейдерам обмінювати криптовалюти безпосередньо між собою, зберігаючи контроль над своїми активами без необхідності передавати їх стороннім організаціям.

Однак, незважаючи на більшу автономність і прозорість транзакцій на DEX, існують деякі обмеження, зокрема відсутність підтримки фіатних валют, менша швидкість виконання ордерів і висока складність для нових користувачів. Оскільки транзакції на децентралізованих біржах є публічними в блокчейні, вони забезпечують більшу конфіденційність та безпеку в порівнянні з централізованими біржами. Проте, кожен користувач самостійно відповідає за безпеку своїх активів. Тепер давайте розглянемо плюси та мінуси децентралізованих бірж (DEX). Одним із основних переваг є високий рівень конфіденційності та анонімності. Для торгівлі на таких платформах зазвичай достатньо підключити криптогаманець і підписати транзакцію, без необхідності верифікації особистості або надання особистих даних. Це приваблює користувачів, які цінують приватність і хочуть уникати процедур, типових для централізованих бірж, таких як KYC.

Ще однією суттєвою перевагою є безпека. Оскільки децентралізовані біржі є некастодіальними, користувачі зберігають повний контроль над своїми приватними ключами і, відповідно, над своїми коштами. Це значно знижує ризик втрати активів через злом біржі або несанкціонований доступ до акаунтів. Крім того, DEX не мають централізованої бази даних користувачів, що зменшує ймовірність витоку особистої інформації.

Інтеграція з децентралізованими фінансами (DeFi) - це ще один плюс для DEX. Вони дозволяють користувачам взаємодіяти зі смарт-контрактами та децентралізованими додатками (DApps), що надають різноманітні фінансові послуги, такі як кредитування, депозитні рахунки, пули ліквідності та інші фінансові інструменти [7]. Це відкриває широкі можливості для трейдерів та інвесторів, які хочуть активно використовувати можливості DeFi-сектору.

Проте є й мінуси. По-перше, функціональність DEX на даний момент обмежена. Зазвичай на таких платформах доступна лише базова функція обміну однієї криптовалюти на іншу. Більш складні фінансові інструменти, такі як маржинальні угоди, лімітні ордери, ф’ючерси та опціони, на більшості DEX відсутні, хоча нові платформи починають їх впроваджувати. Крім того, ефективність роботи децентралізованих бірж часто поступається централізованим через проблеми з масштабованістю, з якими стикаються блокчейни, що лежать в основі цих бірж. Це може призводити до затримок у виконанні ордерів і підвищених комісій за транзакції в часи високої навантаженості мережі.

Таким чином, вибір між централізованими та децентралізованими біржами залежить від пріоритетів користувача: якщо важлива висока ліквідність і зручність, централізовані біржі будуть кращим варіантом. Якщо ж користувач віддає перевагу конфіденційності, безпеці та доступу до новітніх фінансових технологій, варто обирати децентралізовані платформи.

## 1.4 Види атак на криптовалютні біржі

Атаки типу DDoS (Distributed Denial of Service) - це один з найбільш поширених видів кібератак, спрямованих на виведення з ладу серверів криптовалютних бірж. Метою таких атак є створення надмірного навантаження на системи, що обробляють запити користувачів, в результаті чого сервери не можуть нормально функціонувати, і доступ до біржі стає неможливим. Зловмисники використовують для цього ботнети - мережі інфікованих комп'ютерів, які без відома їхніх власників здійснюють атаки. Вони направляють величезну кількість запитів на сервери, що призводить до перевантаження і їхнього виходу з ладу. Ці атаки можуть мати серйозні наслідки для криптовалютних бірж. Вони не лише блокують доступ до сервісів на кілька годин або навіть днів, але й можуть завдати великі фінансові збитки. Біржа вимушена витрачати значні ресурси на відновлення нормальної роботи, в той час як користувачі не можуть здійснювати торгівлю або виведення коштів. Крім того, постраждалі біржі ризикують втратити репутацію серед своїх користувачів, що може призвести до відтоку клієнтів.

Прикладом такої атаки була інцидент 2018 року на криптовалютній біржі Bitfinex, коли хакери здійснили масовану DDoS-атаку. Цей напад призвів до того, що біржа була змушена тимчасово припинити торгівлю та обмежити доступ до платформи, що викликало великі труднощі для користувачів. Хоча біржа змогла відновити свою роботу, цей інцидент став яскравим прикладом того, як DDoS-атаки можуть ставити під загрозу стабільність і надійність криптовалютних бірж [8].

Фішинг - це техніка соціальної інженерії, яка використовує обман для того, щоб отримати конфіденційну інформацію користувачів, наприклад, логіни, паролі або фінансові дані. Зловмисники можуть створювати фальшиві вебсайти, які на вигляд абсолютно не відрізняються від оригінальних платформ, або відправляти переконливі електронні листи, що виглядають як офіційні повідомлення від відомих компаній. Користувач, натискаючи на посилання у

таких листах, потрапляє на підроблену сторінку, де його просять ввести особисті дані. Після цього злочинці отримують доступ до облікових записів і можуть вкрасти кошти або здійснити інші шкідливі дії.

Яскравим прикладом фішингової атаки стала кампанія 2019 року, коли криптовалютні користувачі стали жертвами злочинців, які розсилали підроблені листи від Binance. Ці листи виглядали як офіційні повідомлення від біржі і містили посилання на фальшиву сторінку входу. Користувачі, довіряючи листу, переходили за посиланням і вводили свої облікові дані на шахрайському сайті. Як результат, хакери отримали доступ до акаунтів користувачів і вкрали їхні кошти. Така атака показала, наскільки важливо перевіряти джерела повідомлень і бути обережними при введенні особистих даних онлайн.

Атаки через вразливості в смарт-контрактах є однією з найбільш серйозних загроз у сфері криптовалют і блокчейн-технологій. Смарт-контракти - це автономні програми, що працюють на блокчейні та автоматично виконують умови угод між учасниками. Однак навіть незначні помилки чи вразливості в коді можуть стати причиною серйозних фінансових втрат. Зловмисники можуть використовувати ці вразливості для маніпулювання умовами контрактів, що дозволяє їм красти кошти або змінювати умови угод. Це особливо небезпечно в системах, де велика кількість коштів зберігається в смарт-контрактах, і їх використання не завжди піддається моніторингу.

Одним із найбільш відомих прикладів такої атаки стала подія 2016 року, коли була здійснена атака на DAO (Decentralized Autonomous Organization). DAO був одним з перших великих проектів, що використовував смарт-контракти для автоматизації управлінських функцій, зокрема збору коштів для проектів. Хакери знайшли вразливість у коді смарт-контракту, що дозволяла їм здійснювати рекурсивні виклики для зняття коштів. Це дозволило зловмисникам вивести понад $50 млн із DAO. Хоча пізніше частина коштів була повернена, цей інцидент став уроком для всіх учасників криптовалютного ринку і підвищив увагу до безпеки смарт-контрактів [9].

Однією з основних причин таких атак є складність програмування смарт-контрактів, де навіть маленька помилка може мати серйозні наслідки. Важливою стратегією для запобігання таких інцидентів є ретельний аудит смарт-контрактів перед їх розгортанням на блокчейні. Деякі великі криптовалютні проекти використовують спеціалізовані служби безпеки для перевірки коду на можливі вразливості, але навіть це не гарантує повної безпеки. Хакери постійно вдосконалюють свої методи для знаходження слабких місць у коді, що робить проблему захисту смарт-контрактів дуже актуальною.

Атака на DAO також продемонструвала важливість розуміння механізмів роботи смарт-контрактів і їх впливу на фінансові потоки. Відсутність належної перевірки і тестування коду може призвести до великих фінансових втрат для користувачів і інвесторів. З того часу криптовалютні проекти значно покращили свою практику безпеки, але випадок DAO залишається важливим нагадуванням про ризики, що супроводжують використання смарт-контрактів у криптовалютних екосистемах.

Використання "backdoor" (бекдору) для доступу до систем біржі є одним із найнебезпечніших методів атак, оскільки надає зловмисникам прихований доступ до серверів і внутрішніх систем без відома власників біржі. "Backdoor" може бути залишений внаслідок попередніх компрометацій або навмисно інтегрований у систему під час її розробки. Завдяки такому доступу, хакери можуть маніпулювати транзакціями, викрадати кошти користувачів або навіть змінювати умови торгівлі без виявлення. Ці атаки часто можуть залишатися непоміченими тривалий час, що робить їх надзвичайно небезпечними для бірж і їхніх клієнтів.

Типовий приклад такої атаки трапився в 2017 році, коли криптовалютна біржа Youbit була зламаною через бекдори в її системах [10]. Раніше біржа вже зазнавала атак, і в результаті цих компрометацій в її системах залишились незадокументовані шляхи доступу, через які хакери могли здійснювати несанкціоновані транзакції. Цей доступ дозволив злочинцям вкрасти значні суми коштів, що зрештою призвело до закриття біржі. Це сталося через те, що біржа

не виявила бекдори вчасно, і атакувальники могли вільно маніпулювати фінансовими активами користувачів.

Наявність бекдорів є серйозною проблемою, оскільки навіть після відновлення після попередніх атак або оновлення програмного забезпечення, ці шляхи доступу можуть залишатися прихованими і активно використовуватись зловмисниками. Тому важливим етапом у забезпеченні безпеки є регулярні аудити систем і постійний моніторинг для виявлення таких небезпечних доступів. Біржам необхідно запроваджувати політики безпеки, що включають перевірку всіх етапів розробки, тестування та впровадження нових функцій, щоб уникнути потенційних бекдорів. Застосування "backdoor" для несанкціонованого доступу до біржових систем вимагає ретельної уваги до усіх аспектів кібербезпеки. Важливо забезпечити максимальну прозорість в коді та процесах біржі, використовувати шифрування даних і забезпечувати багатоетапну перевірку для доступу до критичних компонентів системи. Навіть якщо зловмисники мають фізичний доступ до серверів або використовують складні технології для залишення бекдорів, регулярне тестування та перевірка всіх систем допоможе виявити будь-які аномалії, що можуть свідчити про порушення безпеки.

Підсумовуючи щодо видів атак на криптовалютні біржі, можна виділити кілька основних загроз, які активно використовуються зловмисниками для отримання несанкціонованого доступу до систем і фінансових активів користувачів. Це атаки типу DDoS, які спричиняють перевантаження серверів і тимчасову недоступність біржі. Фішинг, який використовує підроблені сайти або листи для збору облікових даних користувачів, також є поширеним методом. Окрім того, вразливості в смарт-контрактах та використання бекдорів можуть призвести до серйозних фінансових втрат і зловживань з боку хакерів.

## 1.5 Типові вразливості криптовалютних гаманців

Типові вразливості криптовалютних гаманців можуть серйозно підвищити ризик втрати активів користувачів. Однією з основних вразливостей є недостатній захист приватних ключів. Приватні ключі є основою для доступу до криптовалютних активів, тому їх безпечне зберігання є критичним. Втрата або викрадення приватного ключа може призвести до повної втрати доступу до коштів. Користувачі часто зберігають приватні ключі на своїх комп'ютерах або в онлайн-сервісах, де вони можуть бути викрадені через віруси, хакерські атаки або інші методи. Іншою поширеною уразливістю є недостатнє шифрування та захист файлів. Криптовалютні гаманці можуть містити важливі дані, такі як приватні ключі та паролі, які можуть бути вкрадені, якщо гаманець не захищений належним чином. Наприклад, зберігання гаманця в незашифрованому вигляді на комп'ютері або в хмарному сховищі підвищує ймовірність його компрометації. Хакери можуть використати вразливості в програмному забезпеченні для отримання доступу до цих файлів та викрадення коштів.

Ще однією уразливістю є відсутність багатофакторної автентифікації (2FA). Без додаткових методів захисту, таких як код, що надсилається на мобільний телефон або електронну пошту, зловмисники можуть легко отримати доступ до гаманця, якщо володіють паролем користувача. Багато користувачів не активують цю функцію або використовують слабкі паролі, що робить гаманці вразливими до атак типу "брутфорс" або фішинг-атак. Помилки в розробці програмного забезпечення можуть також призводити до серйозних вразливостей. Багато криптовалютних гаманців - це складні програми, які можуть містити вразливості в коді. Хакери можуть використовувати ці помилки для того, щоб отримати доступ до гаманців або навіть маніпулювати транзакціями. Погано розроблені або недостатньо протестовані програми можуть бути особливо вразливими до експлуатації таких помилок.

Нарешті, фізичні вразливості криптовалютних гаманців, особливо апаратних, також не можна ігнорувати. Хоча апаратні гаманці зазвичай

вважаються більш безпечними через те, що приватні ключі зберігаються в ізольованому середовищі, вони все одно можуть бути вкрадені або пошкоджені в разі фізичного доступу зловмисника. Якщо пристрій втрачений або украдений, відновлення доступу до криптовалют може бути неможливим без резервних копій або паролів.

Ці помилки виникають через кілька основних причин, пов'язаних як із технічними аспектами, так і з людським фактором. Часто розробники криптовалютних гаманців можуть недостатньо уваги приділяти аспектам безпеки під час створення програмного забезпечення. Високий рівень конкуренції на ринку криптовалют може призвести до того, що гаманці розробляються швидко, без належного тестування на вразливості. Це може призвести до того, що в коді з'являються помилки, які можуть бути використані хакерами для злому гаманця.

Деякі розробники не дотримуються кращих практик з безпеки або стандартизованих методів захисту даних. Наприклад, використання слабких методів шифрування або відсутність належного захисту для резервних копій може відкрити двері для атаки. Крім того, неправильне зберігання або обробка приватних ключів може легко призвести до їх викрадення. Тестування програмного забезпечення криптовалютних гаманців часто не охоплює всі можливі сценарії атак або не здійснюється ретельно. Без належного аудиту коду сторонніми безпековими фахівцями або незалежними компаніями, вразливості можуть залишитися непоміченими. Розробники можуть не враховувати всі потенційні загрози, зокрема нові техніки атак або вразливості, які з'являються з часом.

Багато користувачів криптовалют не мають достатнього рівня знань про безпеку і не використовують надійні методи захисту, такі як багатофакторну автентифікацію або шифрування. Вони можуть зберігати приватні ключі або паролі в ненадійних місцях, використовувати слабкі паролі або не оновлювати програмне забезпечення гаманця, що робить їх вразливими до атак. Людські помилки, такі як неправильне зберігання паролів чи невміння правильно обирати

налаштування безпеки, також сприяють виникненню вразливостей. Крім того, користувачі можуть бути обмануті фішинговими атаками або іншими методами соціальної інженерії, що веде до того, що зловмисники отримують доступ до їхніх криптовалютних гаманців.

Отже, підсумовуючи, основні причини виникнення помилок у криптовалютних гаманцях пов'язані з низьким рівнем уваги до безпеки під час розробки, недотриманням стандартів захисту, недостатнім тестуванням програмного забезпечення та відсутністю належного аудиту. Крім того, недостатня обізнаність користувачів та людський фактор, такі як помилки в управлінні паролями або соціальні маніпуляції, також сприяють виникненню вразливостей. Усі ці фактори в сукупності можуть призвести до серйозних порушень безпеки та втрати криптовалютних активів. Тому важливо постійно вдосконалювати заходи безпеки та підвищувати обізнаність користувачів.

## 1.6 Статистичний аналіз успішних атак на криптовалютні активи

Статистичний аналіз успішних атак на криптовалютні активи дозволяє виявити тенденції, вразливості та ефективність методів захисту в сфері криптовалют. За останні роки спостерігається збільшення кількості таких атак, що свідчить про зростання інтересу до криптовалютних активів та відповідно до можливостей їхнього незаконного отримання. Статистичні дані показують, що фішинг є найбільш поширеним методом атак на криптовалютні активи, займаючи близько 35% від загальної кількості атак. Фішинг часто здійснюється через підроблені вебсайти або електронні листи, що виглядають як офіційні повідомлення від криптовалютних бірж. Користувачі, потрапляючи на ці сайти, вводять свої облікові дані, що дозволяє зловмисникам отримати доступ до їхніх рахунків і активів.

DDoS-атаки, які становлять близько 20% атак, також є одними з найпоширеніших методів. Вони орієнтовані на виведення з ладу серверів криптовалютних платформ, що спричиняє тимчасове припинення доступу до

послуг біржі. Такі атаки можуть створити значні перешкоди для трейдерів та знизити довіру до платформи, хоча безпосередньо не призводять до викрадення коштів. Ще однією важливою категорією атак є зломи через вразливості в смарт-контрактах і на платформах обміну, що займають приблизно 25% випадків. Зловмисники використовують помилки в коді смарт-контрактів або вразливості на біржах для викрадення криптовалютних активів [11]. Ці атаки можуть мати серйозні фінансові наслідки, оскільки зловмисники можуть отримати доступ до великих сум, що знаходяться на платформах. Інші методи, такі як атаки через бекдори або на системи KYC, менш поширені, але часто є більш руйнівними, оскільки дозволяють зловмисникам отримувати доступ до внутрішніх систем або обходити процеси перевірки особистості.

Біржі, гаманці та платформи децентралізованих фінансів (DeFi) є основними мішенями для зловмисників, оскільки вони зберігають значні суми в криптовалюті та надають доступ до широкого спектра фінансових операцій. За перші два квартали 2023 року було зафіксовано понад 30 атак на криптовалютні біржі, що призвело до серйозних фінансових втрат для користувачів і самих платформ. Ці атаки, зокрема через фішинг, DDoS-атаки та зломи через вразливості в смарт-контрактах, показують, що криптовалютні біржі залишаються вразливими та привабливими цілями для хакерів.

Платформи DeFi також стали об'єктами численних атак, і за цей же період було зафіксовано понад 10 атак на ці платформи, в результаті яких втратилися десятки мільйонів доларів. Децентралізовані платформи мають складнішу структуру, що іноді робить їх більш вразливими до зловмисників, котрі експлуатують недоліки в коді смарт-контрактів або маніпулюють з ліквідністю. Це підкреслює важливість постійного вдосконалення безпеки в криптовалютних системах та захисту активів користувачів від потенційних загроз.

Атаки через вразливості в смарт-контрактах є одними з найсерйозніших загроз для криптовалютних платформ. Вони зазвичай виникають через недостатньо ретельне тестування коду або через невірно налаштовані функції, що дозволяють хакерам маніпулювати або викрадати кошти. Прикладом такої

атаки є інцидент 2021 року, коли платформа Poly Network стала жертвою атаки через вразливості в її смарт-контрактах. Внаслідок цього було викрадено понад $600 млн, що є одним з найбільших випадків крадіжки на криптовалютних платформах за всю історію.

Динаміка розвитку атак на криптовалютні платформи показує значне зростання кількості інцидентів після 2020 року. Це пояснюється ростом популярності криптовалют серед інвесторів та спекулянтів, що привернуло до цієї сфери більше уваги з боку зловмисників. За даними аналітиків, кількість атак зросла на 40% з 2021 року, що є відображенням зростання обсягів ринку криптовалют і збільшення інтересу до цього виду інвестицій. Міжнародний контекст атак також вказує на те, що найбільша кількість інцидентів відбувається в країнах з розвиненими фінансовими системами. США, Японія, Південна Корея та Великобританія є основними цілями для атак на криптовалютні платформи, оскільки ці країни мають найбільші ринки криптовалют і значну кількість користувачів. Однак, зловмисники все частіше використовують методи анонімізації, такі як Tor і криптовалюти з високим рівнем анонімності, щоб уникати відстеження і обходити національні безпекові та законодавчі бар'єри.

У 2024 році кібератаки на криптовалютні платформи значно посилилися як в Україні, так і в усьому світі. Глобально було зафіксовано понад 300 хакерських інцидентів, що призвели до втрат на суму близько $2,2 мільярда, що на 21% більше порівняно з попереднім роком. Це вже четвертий рік поспіль, коли втрати від таких атак перевищують $1 мільярд. В Україні ситуація також загострилася. Урядова команда реагування на комп’ютерні надзвичайні події CERT-UA у 2024 році опрацювала 4315 кіберінцидентів, що на 69,8% більше, ніж у 2023 році. Хоча конкретні дані щодо атак на українські криптовалютні платформи обмежені, загальне зростання кіберактивності вказує на підвищену загрозу для цього сектору [12].

Серед найбільших глобальних інцидентів 2024 року виділяється злам японської біржі DMM Bitcoin у травні, під час якого було викрадено 4502,9 BTC (приблизно $305 мільйонів). Також значних втрат зазнала індійська платформа

WazirX, що призвело до призупинення виведення коштів. Децентралізовані фінансові протоколи (DeFi) залишаються основною мішенню для хакерів, на них припадає понад 51% атак. Однак у другому та третьому кварталах 2024 року спостерігалася тенденція переключення уваги зловмисників на централізовані платформи, що пов'язано з концентрацією активів на цих платформах.

Зростання вартості криптовалют, зокрема біткоїна, який перевищив позначку $100 000 у 2024 році, зробило цей сектор ще привабливішим для кіберзлочинців. Крім того, використання штучного інтелекту сприяло підвищенню складності та ефективності шахрайських схем, таких як "pig butchering", де зловмисники встановлюють довгострокові відносини з жертвами для виманювання коштів. У відповідь на ці загрози, українські компанії все частіше звертаються до платформ оцінки кібербезпеки, таких як BitSight та Phantom, оскільки низький рейтинг кібербезпеки може негативно вплинути на бізнес та співпрацю з міжнародними партнерами. Загалом, 2024 рік продемонстрував зростання кількості та складності атак на криптовалютні платформи, що підкреслює необхідність посилення заходів кібербезпеки та міжнародної співпраці для протидії цим загрозам.

Отже, підсумовуючи статистику атак на криптовалютні платформи, можна зазначити, що найбільш поширеними загрозами є фішинг, DDoS-атаки та зломи через вразливості в смарт-контрактах. Зростання популярності криптовалют і збільшення інтересу до них серед інвесторів призвело до 40% зростання кількості атак після 2021 року. Крім того, найбільше атак фіксується в країнах з розвиненими фінансовими системами, такими як США, Японія, Південна Корея та Великобританія, хоча анонімізація атакуючих ускладнює боротьбу з такими злочинами.

**Висновки за розділом 1**

Враховуючи аналіз основних загроз і технічних аспектів атак на криптовалютні біржі та гаманці, можна зробити висновок, що найпоширенішими

методами зловмисників є фішинг, DDoS-атаки та експлуатація вразливостей у смарт-контрактах. Криптовалютні платформи, гаманці та платформи децентралізованих фінансів (DeFi) залишаються привабливими цілями для зловмисників через величезні фінансові обороти та недосконаліть багатьох систем безпеки. Незважаючи на постійне вдосконалення протоколів безпеки, зловмисники успішно використовують недоліки в дизайні систем та їхній недостатній захист, що призводить до значних фінансових втрат. Зростання популярності криптовалютного ринку після 2020 року сприяло збільшенню кількості атак на платформи, що ставить ще більшу відповідальність на операторів криптовалютних бірж та гаманців щодо впровадження ефективних заходів безпеки. Це також показує, що міжнародне співробітництво та посилення регулювання у цій сфері необхідні для зниження ризиків, пов'язаних з атакуючими групами, які використовують методи анонімізації для обходу національних бар'єрів.

# РОЗДІЛ 2
# МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КРИПТОВАЛЮТНИХ БІРЖ ТА ГАМАНЦІВ

## 2.1 Механізми ідентифікації користувачів на криптобіржах

Ідентифікація користувачів на криптовалютних біржах є важливим етапом для забезпечення безпеки та дотримання міжнародних регуляторних норм. Вона здійснюється через процедури Know Your Customer (KYC) та Anti-Money Laundering (AML), які допомагають запобігати фінансовим злочинам, шахрайству та відмиванню грошей. Завдяки цим механізмам біржі можуть перевіряти особу користувача, його фінансові операції та відповідність вимогам законодавства [13].

Перший рівень ідентифікації відбувається під час реєстрації на платформі. Користувач створює обліковий запис, вказуючи e-mail або номер телефону, а потім проходить первинну автентифікацію. Для посилення безпеки криптобіржі впроваджують двофакторну аутентифікацію (2FA) через Google Authenticator або SMS-коди. Це зменшує ризик несанкціонованого доступу до акаунта та захищає активи користувачів. Наступний етап - верифікація особистості (KYC), яка є обов’язковою для більшості криптобірж. Користувач має надати персональні дані, такі як повне ім’я, дату народження та країну проживання. Потім потрібно завантажити документи, що підтверджують особу (паспорт, ID-картку або водійське посвідчення), а також зробити селфі з документом або пройти відеоверифікацію. Деякі платформи застосовують біометричні методи, наприклад, розпізнавання обличчя.

Для боротьби з відмиванням грошей та фінансуванням тероризму криптобіржі впроваджують AML-процедури. Вони включають аналіз документів, перевірку історії транзакцій та моніторинг джерел коштів. Біржі можуть використовувати спеціальні алгоритми та бази даних (наприклад,

Chainalysis, Elliptic) для виявлення підозрілих операцій. Якщо система фіксує аномальні транзакції, користувачеві може бути запропоновано додатково підтвердити джерело доходу.

Окрім перевірки документів, біржі застосовують поведінковий аналіз для підвищення рівня безпеки. Вони відстежують IP-адреси, геолокацію, пристрої, з яких здійснюється вхід, та шаблони фінансової активності. У разі входу з незвичного місцезнаходження або здійснення великих фінансових переказів система може вимагати повторного проходження верифікації. Це дозволяє знизити ризик шахрайства та зломів акаунтів. Залежно від рівня верифікації криптобіржі встановлюють різні обмеження на депозити та виведення коштів. Наприклад, користувачі з базовою реєстрацією можуть проводити лише невеликі операції, а для повного доступу до всіх функцій платформи необхідно пройти повний KYC-процес. Таким чином, система ідентифікації на криптобіржах поєднує зручність для користувачів і дотримання міжнародних стандартів безпеки.

Найбільш поширений спосіб ідентифікації користувачів на криптобіржах - це процедура Know Your Customer (KYC), яка включає кілька етапів. Зазвичай біржі вимагають наданих особистих даних, таких як ім’я, дата народження, країна проживання, а також завантаження офіційних документів, наприклад, паспорта або ID-картки. Цей процес є стандартом для більшості платформ, адже він відповідає вимогам регулювання та допомагає зменшити фінансові злочини, такі як відмивання грошей та фінансування тероризму. Другим важливим елементом є двухфакторна аутентифікація (2FA), яка є важливим інструментом безпеки на багатьох біржах. Після реєстрації користувача на платформі, необхідно налаштувати 2FA, що може бути через SMS або додаток Google Authenticator. Це додає додатковий рівень захисту облікових записів і є дуже поширеним на всіх великих криптобіржах. Завдяки цим двом механізмам — KYC та 2FA - криптобіржі можуть забезпечити достатній рівень безпеки і одночасно виконувати вимоги законодавства, що дозволяє їм працювати в багатьох країнах.

## 2.2 Використання токенів доступу для безпечної аутентифікації

Токенова автентифікація - це процес безпеки, при якому доступ користувача надається на основі дійсного токена, а не лише за допомогою імені та пароля. Токени є унікальними, зашифрованими фрагментами даних, які функціонують як тимчасові облікові дані для доступу. Цей метод автентифікації додає додатковий рівень безпеки, дозволяючи уникнути постійного введення імені користувача та пароля при кожному запиті. Після успішної автентифікації система генерує токен, який користувач використовує для подальших запитів. Перевіривши токен, система може підтвердити особу користувача та забезпечити доступ відповідно до дійсності токена.

Процес токенової автентифікації включає кілька етапів: Користувач вводить своє ім’я та пароль для доступу до системи або додатку. Після успішної автентифікації система генерує токен для користувача - довгий рядок випадкових символів, який криптографічно підписується для збереження цілісності. Користувач додає токен до запитів на ресурси або дані, зазвичай через заголовки запиту або параметри URL. Система перевіряє токен на дійсність та автентичність, зокрема перевіряє цифровий підпис токена і порівнює його з секретним ключем. Якщо токен є дійсним і не вийшов із терміну дії, користувач отримує доступ до запитуваних ресурсів або даних.

Автентифікація за токенами має ряд переваг порівняно з традиційною автентифікацією за допомогою імені користувача та пароля. Однією з головних переваг є підвищена безпека: токени не зберігають чутливу інформацію, таку як паролі, що знижує ризик їх крадіжки або несанкціонованого доступу. Крім того, токени можуть бути видані з конкретними дозволами або обсягами доступу, що дозволяє більш точно контролювати доступ до різних ресурсів.

Також, автентифікація за токенами забезпечує безсесійність та масштабованість. Оскільки сервер не зберігає жодної інформації про сеанс, це дозволяє легше масштабувати застосунки та розподіляти автентифікацію між кількома серверами. Токени також можуть бути використані для впровадження

механізму єдиного входу (SSO), що дає змогу користувачам автентифікуватися один раз і отримувати доступ до кількох сервісів без необхідності повторно вводити свої облікові дані.

Головною перевагою використання токенів доступу для безпечної автентифікації є підвищена безпека. Токени не містять чутливих даних, таких як паролі, що робить їх менш вразливими до крадіжок або несанкціонованого доступу. Окрім того, токени можуть мати обмежений термін дії, що зменшує ймовірність їх використання у разі компрометації. Це дозволяє здійснювати більш точний контроль доступу, а також забезпечує зручність у вигляді безсесійної автентифікації та масштабованості системи.

Однак головним недоліком є можливість компрометації токена, якщо він не буде належним чином захищений. Наприклад, якщо токен потрапить до зловмисників через вразливості в програмному забезпеченні або неналежне зберігання на стороні користувача (наприклад, в браузері чи мобільному додатку), він може бути використаний для отримання несанкціонованого доступу. Це вимагає ретельного управління токенами, таких як їх своєчасне оновлення або відзив у разі підозри на компрометацію. Однак для ефективної реалізації автентифікації за токенами важливо ретельно враховувати аспекти, як термін дії токенів, управління ключами шифрування та обмеження доступу. Поєднуючи цей метод з іншими заходами безпеки, такими як HTTPS та багатофакторна автентифікація, організації можуть значно підвищити рівень захисту своїх систем і зменшити ризики несанкціонованого доступу.

## 2.3 Особливості безпечного підключення до платформ через API

Безпечне підключення до платформ через API (інтерфейс програмування додатків) є критично важливим для забезпечення конфіденційності, цілісності та доступності даних. Основні особливості безпечного підключення включають:

1. Аутентифікація та авторизація. Для забезпечення безпеки підключення до API необхідно використовувати надійні механізми аутентифікації. Один з

найбільш поширених методів - це використання токенів доступу, таких як OAuth 2.0, які дозволяють підтвердити особу користувача чи додатка без необхідності передавати чутливі дані, як паролі. Авторизація дозволяє контролювати доступ до конкретних ресурсів або функцій API відповідно до прав користувача чи додатка.

2. Шифрування даних. Для захисту даних, що передаються між клієнтом і сервером, важливо використовувати шифрування, зокрема протокол HTTPS (SSL/TLS) [14]. Це гарантує, що передані дані будуть захищені від прослуховування або зміни під час передачі, знижуючи ризик атак типу "man-in-the-middle" (MITM).

3. Валідація введених даних. Щоб уникнути атак через введення шкідливих даних (наприклад, SQL-ін'єкцій чи XSS), важливо валідувати всі вхідні запити до API. Валідація даних дозволяє переконатися, що лише коректні і безпечні запити обробляються сервером.

4. Обмеження доступу та моніторинг. Використання лімітів запитів (rate limiting) допомагає запобігти атакам на API, таким як відмова в обслуговуванні (DoS) або надмірне навантаження на сервер. Також важливо вживати заходів моніторингу для виявлення підозрілої активності та вчасного реагування на можливі загрози.

5. Аудит та журналювання. Ведення журналів доступу до API дозволяє організаціям відслідковувати, хто, коли і як використовує API. Це дає змогу виявляти потенційні вразливості або неправильне використання API, а також виконувати аудит і перевірки безпеки для запобігання витоку або зловживанню даними.

Особливість безпечного підключення до платформ через API полягає в комплексному підході до захисту даних і доступу. Використання надійної аутентифікації та авторизації, наприклад через токени доступу, дозволяє забезпечити контроль за тим, хто має право доступу до ресурсу, без необхідності передавати чутливі облікові дані. Шифрування даних через HTTPS гарантує

захист переданої інформації від перехоплення та змін, що є важливим для запобігання атакам на етапі комунікації між клієнтом і сервером.

Додатково, валідація введених даних і обмеження доступу (rate limiting) є ключовими особливостями для запобігання шкідливим атакам та зловживанням API. Моніторинг і ведення журналів доступу дозволяють своєчасно виявляти підозрілу активність і вживати заходів для її зупинки. Ці заходи гарантують, що API залишається безпечним і ефективним, навіть при великій кількості запитів або підвищених ризиках. Всі ці заходи разом створюють безпечне середовище для підключення до платформ через API, забезпечуючи захист даних, контроль доступу та захист від атак.

## 2.4 Захист від атак на стороні клієнта: рекомендації користувачам

Захист від атак на стороні клієнта є важливою складовою безпеки, особливо коли йдеться про взаємодію з веб-додатками та платформами. Рекомендації щодо захисту від атак на стороні клієнта:

1. Використовуйте складні паролі та двофакторну автентифікацію (2FA). Використання простих або однакових паролів для кількох акаунтів збільшує ризик їх злому. Тому важливо створювати складні паролі, які включають комбінації великих і малих літер, цифр та спеціальних символів. Також потрібно обов'язково активувати двофакторну автентифікацію (2FA) для кожного важливого облікового запису. Це додає додатковий рівень захисту, оскільки навіть якщо зловмисник отримає ваш пароль, йому все одно потрібно буде пройти додаткову перевірку (наприклад, через код, надісланий на мобільний телефон або через додаток-генератор коду). Це знижує ймовірність несанкціонованого доступу до акаунтів.

2. Регулярно оновлюйте програмне забезпечення та додатки. Багато атак стають можливими через вразливості в старих версіях програмного забезпечення. Розробники постійно випускають оновлення для усунення виявлених вразливостей, тому регулярне оновлення операційних систем,

браузерів і додатків допомагає захистити вас від новітніх загроз. Встановлення лише офіційних оновлень від розробників дозволяє запобігти зараженню шкідливим програмним забезпеченням, яке може використовувати застарілі вразливості.

3. Обмежуйте доступ до особистої інформації. Особисті дані є основною ціллю для зловмисників. Фішингові атаки, в яких шахраї намагаються отримати ваші чутливі дані, працюють за рахунок введення вас в оману. Уникайте розголошення персональної інформації на незнайомих або сумнівних сайтах. Перевіряйте, чи є сайт захищеним (перевіряючи наявність HTTPS у адресі сайту), щоб убезпечити себе від шахрайських ресурсів. Крім того, намагайтеся уникати введення особистих даних через незахищені мережі, наприклад, у громадських Wi-Fi точках.

4. Використовуйте антивірусні програми та фаєрволи. Антивірусні програми допомагають виявляти і нейтралізувати шкідливе програмне забезпечення до того, як воно завдасть шкоди. Вони регулярно перевіряють комп'ютер на наявність вірусів та інших загроз. Фаєрволи, у свою чергу, контролюють мережевий трафік і блокують з'єднання з підозрілими ресурсами або шкідливими сайтами. Вони додають додатковий рівень захисту, знижуючи ризик атак, які можуть відбутися через інтернет-з'єднання.

5. Бережіть від сесійних атак. Сесійні атаки, зокрема, атаки типу "міжсайтове підроблення запитів" (CSRF) або "викрадення сеансу" (session hijacking), можуть призвести до того, що зловмисник отримає доступ до вашого акаунту, якщо він залишиться відкритим на іншому пристрої чи після тривалого часу бездіяльності. Завжди виходьте з акаунтів, коли закінчите сеанс, особливо якщо використовуєте публічні або спільні комп'ютери. Це запобігає можливості для зловмисників здійснити несанкціоновані дії. Також не зберігайте паролі в браузерах без відповідної безпеки - використовуйте менеджери паролів для безпечного зберігання і шифрування ваших облікових даних.

Ці рекомендації допоможуть вам захистити себе від численних кіберзагроз, зберігаючи конфіденційність особистих даних і забезпечуючи додаткову безпеку при роботі в інтернеті.

## 2.5 Моделі сегментації доступу для криптовалютних платформ

Моделі сегментації доступу для криптовалютних платформ визначають, хто і як може взаємодіяти з ресурсами системи на різних рівнях безпеки. Це є важливим аспектом для забезпечення конфіденційності, цілісності та доступності даних, а також для захисту від несанкціонованого доступу.

Рольова модель доступу (Role-Based Access Control, RBAC). Це одна з найбільш поширених моделей, яка передбачає, що доступ до ресурсів платформи визначається ролями користувачів. Кожен користувач або група користувачів отримує певну роль (наприклад, адміністратор, трейдер, клієнт), і на основі цієї ролі йому надаються або обмежуються доступи до різних частин платформи. Наприклад, адміністратор може мати доступ до всіх функцій, включаючи управління користувачами та налаштуваннями безпеки, тоді як звичайний користувач може здійснювати тільки операції купівлі-продажу.

Переваги: Спрощує управління доступом для великої кількості користувачів. Забезпечує чітке розмежування функцій і доступів. Легко налаштовується і масштабовується. Недоліки: Може бути недостатньо гнучкою для складних платформ з різними рівнями доступу.

Модель на основі атрибутів (Attribute-Based Access Control, ABAC). У цій моделі доступ визначається на основі конкретних атрибутів користувача, ресурсу або середовища (наприклад, час доби, місце розташування, статус користувача тощо). ABAC дозволяє більш гнучко регулювати доступ на основі множини умов, що надає більш точний контроль доступу до криптовалютних активів. Переваги: Високий рівень гнучкості і точності в контролі доступу. Можна комбінувати різні атрибути для більш детальної настройки доступів.

Недоліки: Складність у налаштуванні та управлінні. Вимагає додаткових ресурсів для адміністрування та моніторингу.

Модель на основі політик (Policy-Based Access Control, PBAC). PBAC використовує політики безпеки, щоб визначити, хто і як може взаємодіяти з системою. Політики можуть бути орієнтовані на різні критерії, такі як тип операцій (наприклад, депозит, виведення коштів, торгівля), часові обмеження або інші умови.

Це дозволяє криптовалютним платформам гнучко адаптувати доступ до користувачів, враховуючи різні фактори ризику. Переваги: Дозволяє створювати складні і адаптивні правила доступу. Легко інтегрується з іншими механізмами безпеки, такими як багатофакторна автентифікація. Недоліки: Складність у визначенні та адмініструванні політик. Потрібно регулярно оновлювати політики для забезпечення актуальності та безпеки.

Модель на основі часових обмежень (Time-Based Access Control, TBAC). У рамках цієї моделі доступ обмежується лише в певні години або дні тижня. Для криптовалютних платформ це може бути корисно, наприклад, для обмеження виведення коштів або виконання операцій у час, коли здійснюється перевірка безпеки або на час, коли підвищується ймовірність атак. Переваги: Допомагає знижувати ризики, пов’язані з несанкціонованим доступом у неактивні години. Ідеально підходить для платформ, які мають регулярні технічні перерви або перевірки безпеки. Недоліки: Обмежує гнучкість користувачів, особливо при міжнародному використанні. Вимагає додаткового налаштування і підтримки.

Модель доступу на основі контексту (Context-Aware Access Control). Ця модель визначає доступ до ресурсів в залежності від контексту, у якому здійснюється запит на доступ. Контекст може включати фактори, такі як тип пристрою (мобільний телефон або комп'ютер), мережа (VPN чи публічний Wi-Fi), географічне розташування та інші параметри. На криптовалютних платформах це дозволяє підвищити безпеку, контролюючи доступ з ненадійних джерел. Переваги:Знижує ймовірність атак з ненадійних джерел. Покращує рівень безпеки за рахунок урахування додаткових факторів, таких як географічне

місце. Недоліки: Складність в реалізації та підтримці в умовах динамічних змін користувацького середовища.

Усі ці моделі мають свої специфічні переваги і недоліки. Вибір оптимальної моделі залежить від рівня безпеки, вимог до масштабованості і гнучкості, а також від ресурсів, доступних для адміністрування платформи [15]. Часто платформи комбінують кілька моделей, щоб забезпечити більш високий рівень захисту і гнучкість доступу.

## 2.6 Автоматизація моніторингу підозрілої активності

Автоматизація моніторингу підозрілої активності - це процес використання спеціалізованих програмних інструментів і алгоритмів для автоматичного виявлення, аналізу та реагування на підозрілі чи аномальні дії в системах, мережах або платформах. Це включає в себе постійний аналіз даних про активність користувачів, транзакцій або системних запитів для виявлення потенційних загроз або відхилень від нормальної поведінки, які можуть свідчити про злочинну або шкідливу активність.

Основною метою автоматизації є зниження часу реакції на загрози, зменшення людського втручання та забезпечення більш високої ефективності моніторингу. Такі системи можуть використовувати різні технології, такі як машинне навчання, аналіз великих даних (big data), штучний інтелект та правила для ідентифікації аномалій. Вони можуть автоматично зупиняти підозрілі операції, надсилати попередження адміністраторам або навіть ініціювати захисні заходи, якщо визначають потенційну загрозу (наприклад, блокування доступу до акаунтів або транзакцій).

Автоматизація моніторингу підозрілої активності включає кілька способів, які використовують різні технології та підходи для виявлення аномальних або потенційно небезпечних дій у системах. Аналіз аномалій (Anomaly Detection).Використовуються алгоритми машинного навчання для визначення відхилень від нормальної поведінки користувачів чи системи. Якщо відбувається

транзакція чи дія, що не відповідає зазвичай поведінці конкретного користувача або шаблону, система автоматично маркує її як підозрілу. Наприклад, якщо користувач зазвичай проводить транзакції на невеликі суми, а раптово здійснює великі перекази, система може позначити це як аномалію і надіслати попередження.

Аналіз поведінки користувачів (User Behavior Analytics, UBA). Цей метод фокусується на вивченні звичайної поведінки користувачів на платформі і автоматично виявляє відхилення. Він базується на алгоритмах, які збирають та аналізують метадані щодо дій користувачів (час входу, частота транзакцій, географічне місцезнаходження тощо). Якщо система виявляє, що певний користувач здійснює операції, яких зазвичай не робить, наприклад, авторизацію з незвичного місця або вночі, система може запустити підозрілість.

Використання правил та алгоритмів на основі поведінки. Створення правил для моніторингу певних подій чи транзакцій (наприклад, великі суми, високий рівень активності за короткий період, підозрілі IP-адреси). Це один із найбільш простих способів автоматизувати моніторинг. Наприклад, правило може бути таким: "Якщо транзакція перевищує 10 000 доларів і здійснюється з невідомого IP, відправте попередження адміністраторам". Такі правила можна комбінувати для більш точного виявлення підозрілих дій.

Системи виявлення вторгнень (Intrusion Detection Systems, IDS). Ці системи постійно аналізують мережеву активність для виявлення ознак вторгнення або небажаної діяльності. Автоматизація моніторингу на основі IDS дозволяє виявляти та реагувати на потенційні загрози в режимі реального часу.Наприклад, IDS може виявити аномальні пакети даних або спроби несанкціонованого доступу до системи.

Автоматизовані процеси відповідей на інциденти (Security Orchestration, Automation, and Response, SOAR). Це система автоматизації, яка не тільки виявляє підозрілу активність, а й може автоматично здійснювати реакцію на інцидент. Наприклад, якщо виявлена спроба несанкціонованого доступу або підозріла транзакція, система може автоматично заблокувати користувача або

відкласти транзакцію до подальшої перевірки. SOAR дозволяє інтегрувати різні інструменти безпеки та автоматизувати процеси реагування на інциденти [16].

Моніторинг транзакцій у реальному часі. На фінансових платформах, таких як криптовалютні біржі, автоматизація моніторингу транзакцій у реальному часі дозволяє своєчасно виявляти шахрайські або нелегальні операції. Цей підхід використовує алгоритми, які порівнюють кожну нову транзакцію з попереднім шаблоном транзакцій користувача або історичними даними.

Якщо транзакція виглядає підозрілою (наприклад, відправлена на адресу, яка не була раніше використана), система може запустити автоматичне розслідування або заблокувати операцію. Ці способи допомагають знижувати ризики, пов’язані з кіберзагрозами, автоматизуючи виявлення та реагування на потенційно небезпечну активність в режимі реального часу.

Автоматизація моніторингу підозрілої активності на криптовалютних платформах включає різні методи для своєчасного виявлення та реагування на потенційні загрози. Найбільш ефективним підходом є комбінація різних технологій, таких як аналіз аномалій, аналіз поведінки користувачів (UBA), моніторинг транзакцій у реальному часі і системи виявлення вторгнень (IDS). Аналіз аномалій дозволяє виявляти нові, невідомі загрози, у той час як системи виявлення вторгнень сприяють виявленню зовнішніх атак. За допомогою автоматизації процесів моніторингу можна оперативно реагувати на підозрілі активності, що значно знижує ризики шахрайства або зловмисних дій.

Удосконалення моніторингу за допомогою SOAR дозволяє не тільки виявляти загрози, а й автоматично вживати заходів для їх нейтралізації. Це особливо важливо для платформ з великим обсягом транзакцій і користувачів, де без своєчасної автоматичної реакції може виникнути великий збиток. Застосування таких методів забезпечує безпечний та ефективний контроль доступу та активності на криптовалютних платформах, що дозволяє організаціям швидко реагувати на потенційні загрози та підтримувати стабільність і надійність своїх систем.

## 2.7 Використання технологій багато рівневого захисту даних

Використання технологій багато рівневого захисту даних є критичним аспектом безпеки в сучасних криптовалютних платформах, оскільки дозволяє знизити ймовірність несанкціонованого доступу або крадіжки чутливої інформації. Багато рівневий захист (multilayer security) передбачає застосування декількох паралельних захисних технологій, кожна з яких виконує окрему функцію для забезпечення цілісності та конфіденційності даних. Такий підхід значно підвищує рівень безпеки системи, оскільки навіть якщо одна з ланок буде скомпрометована, інші залишаються захищеними.

Ключові елементи багато рівневого захисту даних включають:

1. Шифрування даних на кожному рівні. Це один із найважливіших механізмів захисту. У криптовалютних платформах дані користувачів, а також транзакцій, шифруються як при передачі по каналу, так і при зберіганні на сервері. Використовуються протоколи, як SSL/TLS для шифрування переданих даних в реальному часі, та AES для шифрування на рівні зберігання. Це знижує ймовірність того, що навіть при витоку даних сторонні особи зможуть їх прочитати або використати.

2. Багатофакторна автентифікація (MFA). Це ще одна важлива ланка багаторівневого захисту. Для підтвердження особи користувача вимагається не тільки правильний пароль, а й додатковий фактор, як-от код із мобільного додатку або біометричні дані (відбитки пальців або розпізнавання обличчя). Завдяки цьому, навіть якщо зловмисник отримає доступ до пароля, він не зможе увійти без другого рівня захисту. Наприклад, платформи, як Coinbase і Binance, активно використовують MFA для забезпечення безпеки своїх користувачів.

3. Ідентифікація за токенами. Криптовалютні платформи також використовують токени доступу для автентифікації користувачів, що дає додатковий рівень захисту. Токени є унікальними, криптографічно захищеними маркерами, які замінюють паролі для автентифікації в реальному часі. Замість того, щоб користувачам щоразу вводити ім'я та пароль, система видає

одноразовий токен, який користувач має включити у запити. Це робить систему менш уразливою до фішингових атак або витоків паролів.

4. Ізоляція середовищ (sandboxing). Для додаткової безпеки платформи використовують ізоляцію середовищ для різних операцій, що допомагає обмежити потенційний збиток від атак. У разі компрометації одного з середовищ (наприклад, середовище для обробки платежів), інші середовища залишаються захищеними.

5. Моніторинг та аудит. Автоматизовані системи моніторингу можуть відслідковувати підозрілу активність у реальному часі, наприклад, великі суми транзакцій або спроби доступу з незвичних географічних локацій. У разі виявлення такої активності система автоматично ініціює додаткові перевірки або блокує доступ.

Згідно з даними Statista, понад 80% атак на криптовалютні платформи відбуваються через витік облікових даних або використання неефективних методів автентифікації. Це підкреслює важливість використання багаторівневого захисту для забезпечення безпеки. Крім того, дослідження з 2021 року показали, що 92% організацій, які використовують багатофакторну автентифікацію, відзначають значне зниження рівня шахрайства та несанкціонованого доступу до систем. Протягом 2022–2024 років криптовалютні платформи зазнали значних втрат через кіберзлочинність. У 2024 році хакерські атаки та шахрайства призвели до втрат понад $3 мільярди, з яких понад 70% ($2,15 мільярда) становили хакерські атаки, а 30% ($834,5 мільйона) - шахрайства.

Отже, такі цифри підкреслюють необхідність впровадження багаторівневого захисту даних для забезпечення безпеки криптовалютних платформ. Загалом, багаторівневий захист даних у криптовалютних платформах є необхідністю для забезпечення стійкості до різноманітних типів кіберзагроз у сучасномі світі.

## 2.8 Впровадження стандартів безпеки на криптовалютних біржах

Забезпечення інформаційної безпеки є ключовим елементом функціонування сучасних криптовалютних платформ. Через високу вартість активів і постійні спроби зламу, біржі повинні дотримуватися міжнародно визнаних стандартів, які гарантують конфіденційність, цілісність та доступність даних користувачів.

Одним з основних стандартів у сфері інформаційної безпеки є ISO/IEC 27001, який визначає вимоги до створення та підтримки системи управління інформаційною безпекою (ISMS). Його впровадження передбачає оцінку ризиків, управління активами, контроль доступу, криптографічний захист, журналювання подій та постійний моніторинг системи.

Окрім цього, міжнародні компанії часто проходять аудит за стандартом SOC 2 (Service Organization Control), що перевіряє захищеність даних у хмарних середовищах і важливий для бірж, які обробляють великі обсяги транзакцій. Наприклад, Coinbase, Binance та Kraken мають сертифікацію SOC 2, що підтверджує їхню відповідність високим стандартам безпеки [17].

Для платіжної інфраструктури криптобірж також актуальним є стандарт PCI DSS (Payment Card Industry Data Security Standard), який регулює зберігання і обробку платіжної інформації. Binance.US та Coinbase дотримуються цього стандарту, забезпечуючи безпечну обробку платіжних даних користувачів [18].

Впровадження цих стандартів дозволяє платформам мінімізувати кіберзагрози, знизити ймовірність атак соціальної інженерії та підвищити довіру користувачів. Наприклад, впровадження багаторівневого контролю доступу, двофакторної автентифікації, сегментованої мережевої архітектури та віддаленого журналювання вже стали індустріальними стандартами для бірж із високими обсягами торгів.

Що стосується України, національне регулювання сфери криптовалют також активно розвивається. У 2021 році Верховна Рада ухвалила Закон України

“Про віртуальні активи”, який визначає правові основи для діяльності постачальників послуг, пов’язаних з обігом віртуальних активів [19]. Проте на момент написання цієї роботи закон ще не набрав чинності, оскільки потребує додаткових підзаконних актів та механізмів реалізації. Водночас, його прийняття є важливим кроком до інтеграції українського ринку в міжнародну криптовалютну екосистему.

Таким чином, впровадження міжнародних стандартів безпеки, таких як ISO/IEC 27001, у поєднанні з національним законодавчим регулюванням, створює підґрунтя для побудови надійних, прозорих та конкурентоспроможних криптобірж як в Україні, так і у світі.

**Висновки за розділом 2**

Постійне зростання кількості кіберзагроз і підвищення складності атак вимагають від учасників крипторинку застосування як технічних, так і організаційних засобів захисту.

Серед ефективних заходів, що широко впроваджуються провідними криптовалютними платформами, варто відзначити багатофакторну автентифікацію, сегментований контроль доступу, криптографічний захист приватних ключів та системи моніторингу аномальної активності. Автоматизація процесів виявлення загроз на ранніх етапах також дозволяє значно зменшити ризики несанкціонованого доступу до активів.

Особливої уваги заслуговує впровадження міжнародних стандартів, таких як ISO/IEC 27001, SOC 2, PCI DSS, що дозволяють створити цілісну систему управління інформаційною безпекою. Ці стандарти передбачають не лише впровадження технічного захисту, але й формування політик безпеки, управління ризиками та проведення регулярного аудиту, що є ключовими умовами для забезпечення довіри з боку користувачів та партнерів.

Водночас в Україні також вживаються кроки щодо формалізації правового поля для діяльності у сфері віртуальних активів. Прийняття Закону України “Про

віртуальні активи”, навіть попри відсутність повного механізму його реалізації, свідчить про намір держави адаптуватися до міжнародних вимог у сфері кібербезпеки та забезпечити легалізацію цифрових активів у національному правовому полі.

Таким чином, можна констатувати, що впровадження міжнародних стандартів інформаційної безпеки разом із розвитком національного регулювання формує основу для підвищення стійкості криптовалютних платформ до сучасних загроз і сприяє формуванню довіри з боку учасників ринку.

# РОЗДІЛ 3
# ІНТЕГРОВАНА СТРАТЕГІЯ ЗАХИСТУ КРИПТОБІРЖ ТА ХОЛОДНИХ ГАМАНЦІВ З РЕАЛІЗАЦІЄЮ МОДУЛЯ CRYPTOCOLDSHARE

## 3.1 Розмежування між правом доступу до акаунту та реальним контролем над активами

Майже у всіх децентралізованих криптобіржах після автентицікації користувача з'являється можливість здійснювати трнзакції, надсилати запити на вивід коштів або змінювати ключові параметри облікового запису без додаткового підтвердження користувача [20]. Така залежність зазвичай створює високі ризики компроментації облікових даних даних при яких зловмисник одразу після авторизації отримує контроль над всіми криптоактивами.

В межах запропонованої моделі безпеки рекомендується впровадження архітектурного розриву між доступом до ключових активів та доступом до акаунту. Впровадження такого підходу передбачає також побудову окремого принципу нез’єднаних контурів, відповідно якому авторизований доступ більше не дорівнюватиме автоматичному отриманню контролю над фінансами.

Операції з виведення коштів відбуваються виключно через офлайн-процедури підтвердження, що можуть включати мультипідпис, перевірку фізичних носіїв або ручну валідацію seed-фрази.

Завдяки такому підходу відбувається мінімізація ймовірності компроментації віртуальних активів навіть у випадку втрати доступу або зламу облікового запису. Впровадження ізоляції механізмів керування активами в сіру офлайн-зону буде надавати біржі суттєву перевагу у захисті від атак як з боку внутрішніх загроз, так і з боку зовнішніх зловмисників.

## 3.2 Архітектура двостороннього підтвердження при управлінні активами

Сучасні централізовані біржі страждають від системної уразливості, через те, що будь-який повний доступ до акаунту відкриває шлях до виводу всіх активів. З одного боку, адміністратор або зловмисник, який отримав контроль над внутрішньою інфраструктурою, технічно спроможний ініціювати та підписати транзакції.

З іншого боку сам користувач, часто діючи імпульсивно або під впливом соціальної інженерії, також здатен миттєво вивести всі кошти без додаткових бар'єрів. Таким чином, як централізований контроль, так і повна автономія несуть високі ризики. Для усунення цієї подвійної вразливості пропонується новий підхід - двостороннього підтвердження при управлінні активами.

Ключовим принципом є те, що жодна зі сторін не може реалізувати рух активів самостійно. Навіть користувач, маючи повний доступ до особистого кабінету, не спроможний здійснити негайний вивід активів без проходження зовнішнього рівня затвердження, який є нефальсифікованим та ізольованим. Зі свого боку, біржа не зберігає приватних ключів і не має змоги підписати транзакцію без дії користувача, тобто не має доступу до активів.

Технічно це реалізується шляхом розподілу підпису між двома незалежними контекстами: один зберігається на локальному пристрої користувача, а інший не є приватним ключем у класичному розумінні, виступаючи як обмежувальний верифікатор, що накладає політику доступу на рівні мережевого шлюзу.

Таким чином формується система з архітектурно вбудованою недовірою до всіх сторін. Біржа не здатна використовувати віртуальні активи користувача навіть у разі технічного зламу, а користувач не може швидко вивести активи, не пройшовши через ланцюжок підтверджень, який не контролюється повністю з жодного боку. Важливо, що при цьому зберігається функціональна гнучкість: обіг невеликих сум може залишатися доступним із мінімальними затримками,

тоді як операції з високим ризиком обов'язково запускають серію обов’язкових перевірок.

Цей підхід не просто зменшує площу атаки, а фактично змінює логіку володіння активами у централізованих системах. Вперше технічно реалізується те, що в правовій системі називається довірчим управлінням: біржа не володіє коштами, але має обов’язок їх захистити. А користувач -володіє, але не може діяти без механізмів стримування. Саме така динамічна, неієрархічна архітектура є основою для формування нової моделі безпеки криптобірж: не просто холодне/гаряче сховище, а адаптивна среда, де всі дії потребують симетрично обґрунтованої згоди.

### 3.3 Технічна реалізація архітектури асиметричного контролю активами управління

Процес транзакції в системі асиметричного контролю активами управління поділяється на кілька взаємозалежних етапів, кожен з яких належить до окремої контрольної зони: клієнт (користувач), верифікаційна інфраструктура біржі та нейтральна сторона перевірки. Такий поділ включає можливість реалізації транзакції без узгодження щонайменше двох незалежних сторін.

1. Ініціація починається на боці користувача. Він формує запит на виведення активів через інтерфейс біржі. На цьому етапі біржа не має доступу до підпису чи приватного ключа - вона лише створює шаблон (непідписану транзакцію) та шифрує його для передачі користувачам. Цей шаблон завантажується або сканується на холодний-пристрій користувача (наприклад, автономний модуль з ключем), який завершує транзакцію криптографічного підпису в повній ізоляції від мережі.

2. Передача транзакцій відбувається назад у середовищі біржі. Однак на цьому етапі транзакція не передається в блокчейн. Вона спочатку потрапляє у внутрішній шлюз перевірки політики (Policy Gateway), який міститься в

окремому DMZ-сегменті. Біржа перевіряє валідність підпису, проте не може модифікувати транзакцію. Далі вмикається механізм "розумної затримки", який активується залежно від суми, адреси, історії користувача та результатів проведеного аналізу (UEBA).

3. При низькому ризику транзакція надходить на розгляд нейтральної сторони - автономного контрольного вузла, який не зберігає приватні ключі та функціонує як зовнішній арбітр. Ві перевіряє цифрові підписи, логи, хеш-трейл і відповідність встановленим політикам. У разі проходження цієї перевірки - генерує дозвіл на публікацію в блоці.

4. Лише після узгодженого дозволу від трьох рівнів (користувач, біржа, нейтральний арбітр) - транзакція передається до транслятора, який передає її в публічну мережу через захищений шлюз. Таким чином, жодна зі сторін - ані користувач, ані біржа, ані нейтральна система - не має повного одноособового контролю над рухом коштів.

Така архітектура забезпечує багаторівневий механізм: навіть якщо обліковий запис користувача буде скомпрометовано, атакувач не отримає доступ до підпису, а у випадку якщо буде скомпрометована біржа - вона не може передавати активи без приватного ключа користувача та дозволу третьої сторони. Ця модель імітує логіку “розподіленого трасту”, де контроль над активами розподілений між сторонами без централізації ризиків [21]. Саме така реалізація забезпечує безпеку цифрових активів на порядок вищу для класичних гарячих або мультипідписних рішень.

## 3.4 Аварійне відновлення доступу через резервні механізми холодного зберігання

Ефективне функціонування криптографічної інфраструктури вимагає не лише безпечного зберігання ключів, а й надійного механізму їх відновлення у випадку втрати, апаратного знищення або несанкціонованого фізичного впливу. У контексті запропонованої системи реалізовано адаптивний підхід до

аварійного відновлення доступу, який ґрунтується на використанні розподіленого криптографічного зберігання, незалежних середовищ та багатоетапної верифікації.

У межах цього підходу застосовується метод Shamir Secret Sharing (SSS) - криптографічна схема розділення секрету, що дозволяє поділити ключову інформацію на декілька фрагментів, з яких лише певна кількість (k від n) необхідна для повного відновлення. У нашому випадку реалізовано варіант поділу ключа на три частини з відновленням при наявності будь-яких двох. Одна частина зберігається локально, друга - у вигляді фізичного носія (QR-коду), третя на ізольованому сховищі із захистом доступу.

Цей механізм надає подвійний рівень захисту, тобто навіть при компрометації одного з компонентів, ключ не може бути реконструйований. В той же час користувач має змогу ініціювати аварійне відновлення через механізм багаторівневої ідентифікації. Запропонована система є унікальною в тому, що схема SSS інтегрована в автономну екосистему без залучення сторонніх серверів чи хмарних сервісів -повністю офлайн та контрольовано користувачем.

Варто наголосити, що більшість сучасних холодних гаманців застосовують централізовані або квазі-централізовані моделі резервного копіювання, які не гарантують належної стійкості до витоку або фізичного захоплення ключового матеріалу. Натомість використання Shamir Secret Sharing у запропонованій моделі є не лише безпечнішим, але й рідкісним у практичній реалізації, особливо з урахуванням мультиформатного зберігання частин та автономного сценарію відновлення. На момент написання цієї роботи подібна реалізація не зустрічається у відкритих комерційних рішеннях, що свідчить про її інноваційність і потенціал до стандартизації.

Отже, запропонований механізм відновлення дозволяє гарантувати неперервність доступу до активів без необхідності створення централізованих сховищ або передачі повноважень третім особам, дотримуючись засад криптографічної стійкості та незалежності користувача у критичних ситуаціях.

### 3.5 Поведінкова модель контролю транзакцій з динамічними обмеженнями ризику

Задля зниження ризику масового або раптового виведення активів з рахунку користувача в рамках запропонованої архітектури реалізується вбудована система постійного моніторингу дій, що формує індивідуальний поведінковий профіль. Метою такого підходу є запобігання сценаріям, за яких компрометація акаунту (наприклад, через фішинг чи витік ключа) дозволяє зловмиснику миттєво вивести всі кошти користувача без логічних обмежень.

Система функціонує як компонент верифікаційного шару та постійно аналізує діапазон дій користувача: частоту входів, об’єм і тип транзакцій, часові шаблони активності, географічну послідовність IP-адрес, прив’язані пристрої та тривалість сесій. На основі цього профілю автоматично встановлюються динамічні ліміти: наприклад, дозволене виведення не більше 10% від загального балансу на добу або обмеження на транзакції після зміни локації.

У разі відхилення від звичного патерну (наприклад, якщо користувач раніше виводив по 2% раз на тиждень, а тепер ініціює одноразове виведення 80%) - транзакція блокується до проходження розширеної перевірки. Це включає додаткову багатофакторну автентифікацію, верифікацію особистості через окремий канал або підтвердження змін локації вручну через службу підтримки [22].

Така система може працювати як розширення стандартного UEBA-модуля, або як окремий сервіс у рамках біржової SOC-архітектури. Технічно моніторинг реалізується через проксі-шлюз, що перехоплює запити користувача й передає їх до поведінкового брокера. Брокер проводить обчислення ризику в реальному часі на основі збереженого профілю та політик. При досягненні порогу спрацьовує Rule-Based Trigger, який блокує транзакцію або знижує її пріоритет в обробці.

На відміну від класичного SIEM, де події аналізуються після інциденту, така модель є попередньо-спрогнозованою, тобто вона модифікує поведінку

системи ще до завершення транзакції. Таким чином, навіть у випадку повного контролю над сесією зловмисник обмежений умовами, які можна змінити лише через додаткове підтвердження.

Архітектурно ця модель підтримує інтеграцію з верифікаційним шлюзом, який стає фінальним етапом. Саме через нього проходять транзакції з високим ризиком або з нестандартними параметрами. Якщо шлюз фіксує спробу ініціації дії з нової країни, нового пристрою або після тривалої неактивності - система автоматично накладає статус очікування, сповіщає користувача та активує процедуру ручного розблокування.

Отже, даний підхід дозволяє не лише відслідковувати потенційні атаки типу "account takeover" або злам через соціальну інженерію, а й ефективно обмежує "одноразове виведення всього балансу", навіть у разі легального входу в акаунт.

Таке рішення є адаптованим до масштабування та може бути реалізоване в рамках існуючої SOC-інфраструктури без кардинальних змін у логіці транзакцій - шляхом валідації запиту через окремий верифікаційний шлюз, підключений до поведінкового аналізатора. Архітектуру контролю транзакцій представлено на рисунку 3.1.

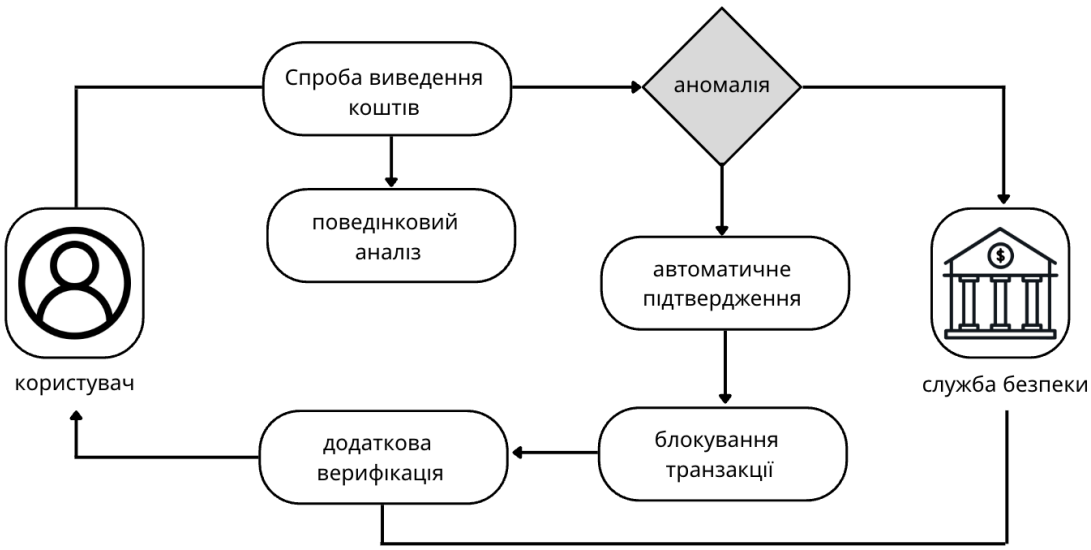


Рисунок 3.1 - Архітектура поведінкового контролю транзакцій

## 3.6 Концепція та архітектура системи CryptoColdShare

У криптовалютних активах seed-фраза (мнемонічна фраза) - це набір із 12 або 24 слів, які є єдиним ключем доступу до приватних ключів користувача. Вона використовується для генерації пари ключів (приватного та публічного) у багатьох гаманцях згідно з протоколами BIP-39/44.

Крім того, втрата або компрометація seed-фрази означає повну втрату доступу до активів. Попри це, більшість користувачів зберігають її у вкрай ненадійний спосіб: на скріншоті, в блокноті на комп'ютері або у хмарі. Усі ці методи мають спільну вразливість - вони централізовані та легко скомпрометовані при атаці на пристрій або обліковий запис.

Система CryptoColdShare пропонує інший підхід - децентралізоване зберігання сид-фрази за допомогою розділення її на три частини. Замість того щоб зберігати весь ключ у єдиній точці, ми розділяємо його за допомогою методу Shamir Secret Sharing, що дозволяє відновити фразу при наявності будь-яких двох частин із трьох. Це забезпечує як відмовостійкість, так і розподілення ризиків (див. табл. 3.1).

Одна частина зберігається у текстовому файлі, інша - у вигляді QR-коду й надсилається у Telegram бот, а третя виводиться у консоль лише один раз, без збереження, для запису вручну на папері. Такий підхід дозволяє уникнути збереження всіх частин в одному цифровому середовищі, і забезпечує багаторівневий захист: цифровий, мережевий та фізичний.

*Таблиця 3.1*

Порівняльна характеристика компонентів системи зберігання seed-фраз

| **Компонент** | **Традиційне зберігання** | **CryptoColdShare** |
|---|---|---|
| **Тип збереження** | Слова (BIP-39) у відкритому вигляді | Зашифрована числова форма через Shamir SSS |
| **Формат сид-фрази** | Цілісна, зберігається одним блоком | Розділена на частини з відновленням по 2 із 3 |

*продовження таблиці 3.1*

| | | |
|---|---|---|
| **Локація зберігання** | Один носій (файл/папір/хмара) | Різні носії (файл, Telegram, фізичний папір) |
| **Шифрування** | Відсутнє або слабке | Основано на криптографічному розділенні (Shamir SSS) |
| **Толерантність до втрат** | Втрата = втрата фрази | Можна втратити 1 частину без наслідків |
| **Передача частини** | Через ризиковані канали (email, фото) | Telegram-бот із захистом приватного каналу |
| **Автономність** | Часто потребує сторонніх сервісів (cloud) | Повністю офлайн, не залежить від сторонніх API |
| **Інтерактивність** | Немає механізмів контролю або верифікації | Сценарії створення/відновлення керуються вручну |

Отже, архітектура CryptoColdShare дає змогу користувачу самостійно вибрати, як зберігати частини - на флешці, у телефоні чи у фізичному сейфі. Таким чином, система пропонує простий, але ефективний механізм посилення безпеки seed-фраз, який можна використовувати як доповнення до апаратних гаманців або як самостійне cold storage рішення[23].

### 3.7 Логіка роботи системи та механізм поділу seed-фрази в CryptoColdShare

Програма CryptoColdShare працює в інтерактивному режимі, дозволяючи користувачу ініціювати процес створення гаманця, ввести власну seed-фразу (яка не зберігається у відкритому вигляді), поділити її на частини за допомогою криптографічного алгоритму та передати ці частини різними каналами у вигляді

числових кодів, а не прямим текстом у вигляді слів, як зазвичай це відбувається при збереженні seed-фрази [24]. Надалі програма також надає можливість відновити повну фразу з будь-яких двох частин, що були збережені раніше, гарантуючи безпечне та резервоване зберігання даних.

CryptoColdShare складається з ряду логічно розподілених модулів, кожен з яких відповідає за окрему функціональність:

- main.py - головний керуючий скрипт. Відповідає за інтерфейс користувача, логіку меню, обробку введення, передачу команд до інших модулів.
- wallet_creator.py - генератор нових фраз (опційно), що може бути використаний для створення seed-фрази за стандартом BIP-39, однак у поточній реалізації фраза вводиться користувачем вручну.
- shamir_tools.py - реалізує алгоритм Shamir Secret Sharing. Перетворює введену фразу в числову форму, розділяє її на три частини з порогом 2 з 3. Забезпечує криптографічну стійкість поділу.
- qr_tools.py - конвертує одну з частин у QR-код, який зберігається у PNG-файл. Також дозволяє зчитувати код у зворотному напрямі для відновлення.
- telegram_tools.py - забезпечує передачу QR-файлу в Telegram-бот. Бот має вбудовану авторизацію по ID користувача і не відповідає публічно, що мінімізує ризики витоку.
- storage.py - відповідає за збереження частин у текстові файли. Забезпечує локальне зберігання частини A на зашифрованому диску або флешці.
- recover_secret.py / main.py - дозволяє вручну ввести будь-які дві з трьох частин і відновити первинну seed-фразу або її числовий еквівалент (якщо декодування неможливе).

Файлова архітектура реалізації компонентів представлена на рисунку 3.2.

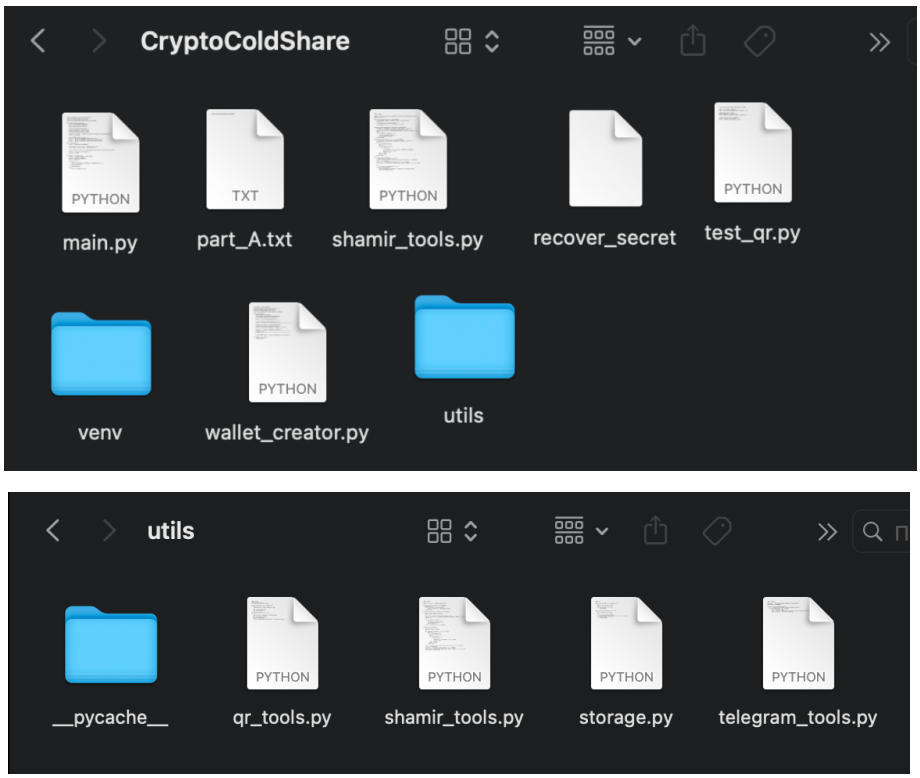


Рисунок 3.2 - файлова архітектура реалізації функціональних компонентів інструменту CryptoColdShare

Сценарій дій користувача:

1. Користувач запускає програму та обирає опцію створення гаманця.
2. Вводить власну seed-фразу (напр., 12 слів).
3. Програма автоматично ділить фразу на 3 частини:

Частина A зберігається у вигляді текстового файлу "part_A.txt", де представлена у числовій формі, сформованій методом Shamir Secret Sharing.

Частина B конвертується у QR-код, який зберігається у файлі "part_B_qr.png" та надсилається в Telegram за допомогою Bot API з авторизацією.

Частина C виводиться безпосередньо в консоль користувача лише один раз - для подальшого ручного запису на папері, без цифрового збереження.

4. Користувач записує частину C вручну на папері та зберігає інші частини окремо.

Меню програми, процес генерації та розподілу seed-фрази в системі CryptoColdShare представлено на рисунках 3.3 та 3.4.

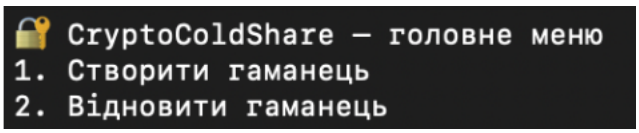


Рисунок 3.3 - Меню програми CryptoColdShare

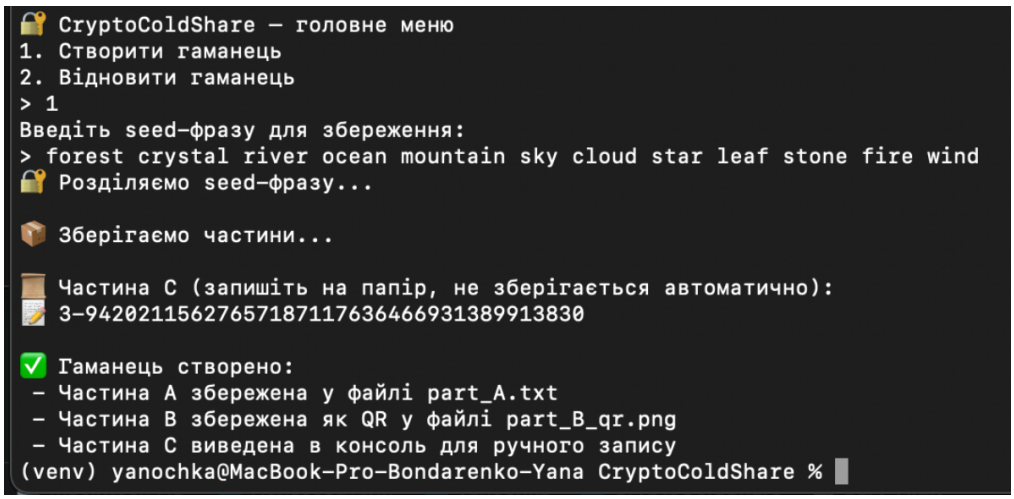


Рисунок 3.4 - Процес генерації та розподілу seed-фрази в системі CryptoColdShare

На зображенні продемонстровано завершальний етап процесу розподілу seed-фрази в системі CryptoColdShare (рис 3.5). Частина C виводиться виключно в термінал - без збереження у файл або будь-яке інше цифрове середовище. Користувач зобов’язаний самостійно зафіксувати цю частину вручну, оскільки після завершення сеансу вона буде втрачена без можливості відновлення.

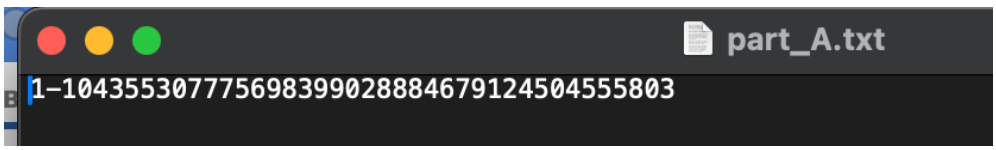


Рисунок 3.5 - Частина A seed-фрази, збережена у текстовому файлі part_A.txt

На скріншоті представлено фрагмент seed-фрази, збережений у текстовому файлі на локальному пристрої користувача. Формат запису включає номер частини (1) та відповідну криптографічну складову, сформовану згідно з алгоритмом Shamir Secret Sharing. Цей файл створюється автоматично і є однією з трьох частин, необхідних для подальшого відновлення повної seed-фрази.

На зображенні представлено Telegram-інтерфейс, через який система CryptoColdShare надсилає частину B розділеної seed-фрази у вигляді QR-коду

(рис 3.6). Цей крок є частиною архітектури децентралізованого зберігання, де кожен фрагмент фрази зберігається у відокремленому середовищі.

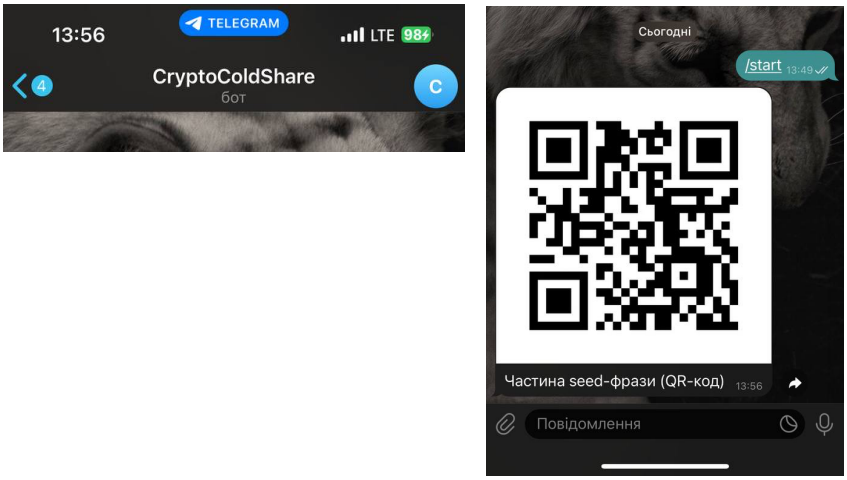


Рисунок 3.6 - Передача частини B seed-фрази у вигляді QR-коду через Telegram-бот

Передача через захищеного Telegram-бота дозволяє уникнути збереження ключової інформації у файловій системі користувача та забезпечує ізольований канал доставки. Навіть у разі компрометації одного із середовищ, повне відновлення seed-фрази залишається неможливим без решти частин. Формат QR-коду також спрощує подальше використання даних для відновлення через інтерфейси ізольованих пристроїв, зберігаючи при цьому криптографічну цілісність переданої інформації.

Отже, варто зазначити, що CryptoColdShare не є повноцінним гаманцем - це інструмент для створення й безпечного зберігання seed-фрази, яка є частиною криптографічної ідентичності. Він може інтегруватися у більші системи зберігання активів як окремий захищений компонент для управління seed-фразами. Тобто, цей інструмент може бути використаний як модуль більшої cold storage-архітектури, що забезпечує додатковий рівень захисту критичних даних.

## 3.8 Процедура відновлення seed-фрази

Процедура відновлення seed-фрази в системі CryptoColdShare реалізована на основі криптографічної схеми Shamir Secret Sharing, яка дозволяє розподілити секрет на декілька фрагментів таким чином, щоб для відновлення було достатньо лише двох із трьох частин. Такий підхід забезпечує стійкість до втрати одного фрагменту, водночас гарантує, що компрометація лише однієї частини не відкриває доступу до повної seed-фрази.

Процес відновлення реалізовано у вигляді окремого режиму, де користувач послідовно вводить дві доступні частини: наприклад, шляхом вибору локального файлу з частиною A та сканування QR-коду з частиною B. Відновлення відбувається в режимі офлайн, без підключення до мережі, що виключає можливість перехоплення даних у момент реконструкції ключа.

На рисунку 3.7 продемонстровано інтерфейс інструменту ZXing Decoder Online, який дозволяє користувачу здійснити декодування QR-коду, що містить одну з частин seed-фрази.

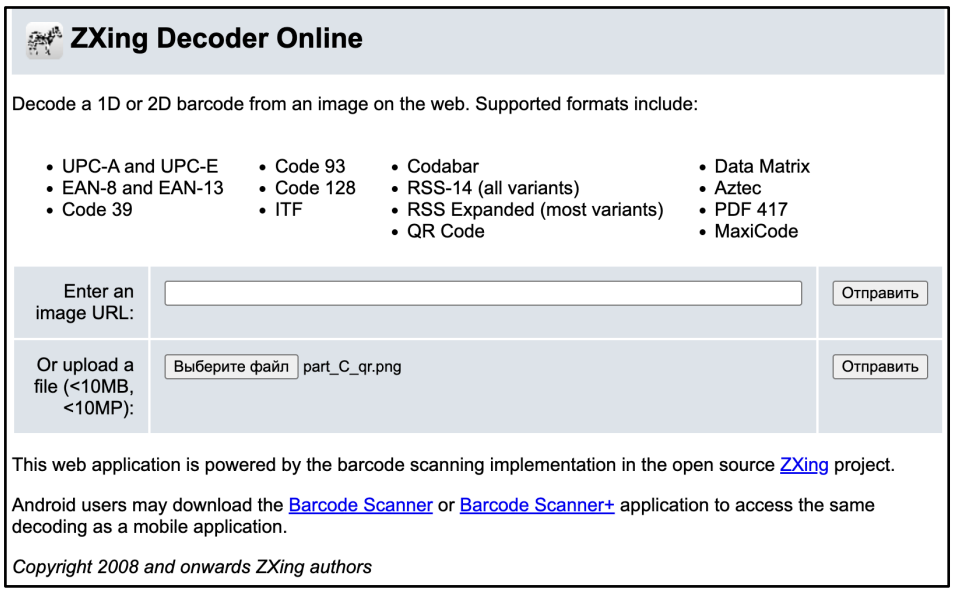


Рисунок 3.7 - Завантаження QR-файлу до вебдекодера ZXing Decoder Online

У даному прикладі обирається файл part_C_qr.png, збережений під час генерації системою CryptoColdShare.

У результаті обробки зображення, вебдекодер виводить числове значення "3–95961029519621752685625844365482948053", що є однією з трьох частин, на які було поділено початкову seed-фразу за схемою Shamir Secret Sharing (рис 3.8).

**Decode Succeeded**

| | |
|---|---|
| Raw text | 3-95961029519621752685625844365482948053 |
| Raw bytes | 40 23 32 d1 09 bb f9 89 27 31 0d 98 3b 58 40 9b<br>ba 3b 3d 78 1a 80 ec 11 ec 11 ec 11 |
| Barcode format | QR_CODE |
| Parsed Result Type | TEXT |
| Parsed Result | 3-95961029519621752685625844365482948053 |

Рисунок 3.8 - Результат декодування QR-коду з частиною seed-фрази

Цей результат підтверджує можливість відновлення критичних даних з графічного носія (QR-коду), що підвищує надійність і зручність аварійного відновлення доступу до криптоактивів у разі втрати одного з інших носіїв.

Інтерфейс вводу частин A та B продемонстровано на рисунку 3.9.

```
🔐 CryptoColdShare — головне меню
1. Створити гаманець
2. Відновити гаманець
> 2
📩 Відновлення seed-фрази
Введіть першу частину (з файла або з паперу): 1-67036910284445215243902785152683556503
Введіть другу частину (з QR або файла): 3-152388106614366867494378088731811021657

🔑 Відновлена seed-фраза:
🧠 forest crystal river ocean mountain sky cloud star leaf stone fire wind
(venv) yanochka@MacBook-Pro-Bondarenko-Yana CryptoColdShare %
```

Рисунок 3.9 - інтерфейс вводу частини A та B

Після успішного введення двох фрагментів система виконує перевірку цілісності даних і формує повну seed-фразу. Результат виводиться в консоль для ручного копіювання - жодна частина не зберігається автоматично. Це означає, що навіть у разі доступу до комп’ютера після завершення сесії - зловмисник не зможе відновити seed-фразу без фізичного доступу до обох частин.

## 3.9 Оцінка ефективності та порівняння з іншими рішеннями

Для визначення практичної цінності розробленого інструменту CryptoColdShare було проведено серію функціональних тестів, що імітують основні сценарії використання: генерація, збереження та відновлення seed-фрази. Система продемонструвала повну працездатність у середовищі macOS із Python 3.11. Моделювання втрати частин seed-фрази підтвердило заявлену стійкість Shamir Secret Sharing до компрометації однієї частини: відновлення було успішним при наявності будь-яких двох із трьох частин.

Особливу увагу приділено оцінці моделі захисту CryptoColdShare порівняно з найпоширенішими cold wallet-рішеннями, зокрема такими як Ledger Nano, Trezor Model T, Casa Keymaster [25]. Основні критерії аналізу включають стійкість до атак, контроль користувача, відсутність централізованих елементів, зручність у використанні та рівень автономності (див. табл. 3.2).

*Таблиця 3.2*

Порівняльний аналіз рішень з безпечного зберігання seed-фраз у cold wallet-середовищах

| **Критерій** | **Ledger Nano / Trezor** | **Casa Keymaster** | **CryptoColdShare** |
|---|---|---|---|
| Зберігання seed-фрази | Локально (у пристрої) | У трьох ключах | Розподілено: файл / QR / папір |
| Централізована частина | Так (фірмовий софт) | Так (cloud-акаунт) | Відсутня |
| Відновлення при втраті частини | Важке / неможливе | Можливе, але централізоване | Легке через будь-які 2 з 3 частин |
| Функціонування офлайн | Частково | Ні | Повністю офлайн |

*продовження таблиці 3.2*

| | | | |
|---|---|---|---|
| Підтримка резервних копій | Обмежено | Так | Так, без хмари |
| Атаки типу SIM-swap / phishing | Можливі | Ймовірні | Неможливі без фізичного доступу |
| Контроль користувача | Частковий | Частковий | Повний |
| Вартість | Висока | Дуже висока (від $250) | Безкоштовно (open-source) |

Таким чином основною перевагою CryptoColdShare є максимальна автономія та незалежність від хмарних чи вендорських рішень, що є критично важливим для користувачів, які прагнуть зберігати активи надійно та без зайвих посередників. Всі процеси - від генерації до відновлення - відбуваються офлайн, що повністю усуває можливість атаки через мережу.

Крім того, значною перевагою є відсутність фінансових витрат, тобто на відміну від апаратних гаманців, що потребують купівлі пристрою, або підписок на хмарні сервіси, CryptoColdShare є повністю відкритим і безкоштовним рішенням. Це робить його доступним для широкого кола користувачів, включно з тими, хто не має змоги інвестувати у дорогі захисні інструменти.

Отже, CryptoColdShare позиціонується як trustless cold wallet-рішення нового покоління, яке не лише усуває ключові недоліки класичних моделей, а й створює умови для масштабованої інтеграції у криптобіржі та корпоративні інфраструктури.

**Висновки до розділу 3**

У третьому розділі було проаналізовано як загальні підходи до захисту криптовалютних бірж та холодних гаманців, так і реалізовано інструмент CryptoColdShare - автономне рішення для децентралізованого зберігання seed-

фрази. Запропонована модель безпеки ґрунтується на принципах сегментації доступу, багаторівневого контролю та фізичного розмежування середовищ.

Основні висновки:

- Ізоляція облікового запису від активів дозволяє уникнути прямого доступу до коштів у разі компрометації користувацького акаунту.
- Використання механізмів двофакторної авторизації, розподіленого підпису та мінімізації єдиного вектора доступу значно підвищує безпеку як з боку клієнта, так і з боку біржових сервісів.
- Впровадження поведінкового аналізу, обмежень виведення та контрольних сценаріїв забезпечує адаптивну реакцію на потенційно шкідливу активність.
- CryptoColdShare довів свою ефективність як trustless cold storage-рішення, що не потребує сторонніх сервісів, працює повністю офлайн і гарантує повний контроль з боку користувача.
- Реалізація алгоритму Shamir Secret Sharing у поєднанні з децентралізованим зберіганням частин seed-фрази (файл, Telegram-бот, паперовий носій) створює додатковий захисний шар та підвищує відмовостійкість.

Таким чином, розроблена модель поєднує перевірені криптографічні алгоритми з практичними інструментами та принципами кібергігієни. CryptoColdShare може бути інтегрований як частина персональної безпеки користувача, так і в складі корпоративної інфраструктури cold storage.

# ВИСНОВКИ

У першому розділі дослідження було проаналізовано поточний стан безпеки криптовалютних бірж та холодних гаманців, зокрема їх вразливості до різноманітних кіберзагроз. Найбільше загрозами страждають централізовані біржі через зберігання коштів на централізованих рахунках, що робить їх привабливими для хакерів. Водночас децентралізовані платформи також мають свої слабкі місця, зокрема недостатній рівень захисту користувацьких гаманців та обмежену здатність для масштабного аудиту. Виявлено, що постійне вдосконалення безпеки є необхідністю, адже з розвитком технологій кіберзагрози постійно змінюються і стають складнішими.

Другий розділ дослідження був присвячений вивченню основних методів захисту, які вже використовуються на криптовалютних платформах і в холодних гаманцях. Одним із найбільш ефективних методів є багатофакторна автентифікація, що додає додатковий рівень захисту облікових записів користувачів. Апаратні гаманці, які зберігають приватні ключі в офлайн-режимі, є одними з найбезпечніших варіантів для збереження криптовалют. Також були розглянуті мультипідписи, які вимагають підтвердження транзакцій кількома сторонами, що підвищує рівень безпеки.

У третьому розділі було досліджено архітектурні принципи захисту криптовалютних бірж і холодних гаманців, а також реалізовано програмний інструмент для безпечного зберігання seed-фрази. Проведено аналіз типових вразливостей, пов’язаних із прямим доступом до активів після автентифікації, та запропоновано механізми їхнього усунення шляхом розмежування контролю між акаунтом і ключовими транзакціями.

Проаналізовано асиметричну модель керування, де підтвердження операцій вимагає багаторівневого офлайн-підпису, нейтральної перевірки та поведінкової валідації. Основною інновацією стала реалізація інструмента CryptoColdShare, що дозволяє розділити seed-фразу на три частини за схемою

Shamir Secret Sharing: текстовий файл, QR-код і ручний запис. Частини передаються різними каналами, не зберігаються централізовано та дозволяють відновити фразу лише при наявності двох із трьох. Усі процеси - створення, збереження, відновлення - реалізовані повністю офлайн.

Інструмент успішно протестований у середовищі macOS із Python 3.11 та продемонстрував високу стійкість до компрометації. У порівнянні з апаратними гаманцями та хмарними рішеннями, CryptoColdShare забезпечує максимальний контроль користувача без фінансових витрат і може використовуватись як незалежний модуль у більш складних архітектурах зберігання криптоактивів.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Когут, Ю. Т. Технології блокчейн та криптовалюта: ризики та кібербезпека / Ю. Т. Когут. – Київ : центр учбової літератури, 2022. – 316 с.

2. How To Use MetaMask Wallet? [Електронний ресурс]. – Режим доступу: https://coinsutra.com/use-metamask-wallet/

3. What Is a DEX (Decentralized Exchange)? [Електронний ресурс]. – Режим доступу: https://www.blockchain.com/learning-portal/lessons/what-is-a-dex-decentralized-exchange

4. Hot Wallets vs. Cold Wallets: Which is Safer for Your Crypto? [Електронний ресурс]. – Режим доступу: https://www.osl.com/hk-en/academy/article/hot-wallets-vs-cold-wallets-which-is-safer-for-your-crypto

5. Keep your Crypto Info safe and secure. – Crypto Cold Wallet Publishing, 2021. – 33 с.

6. What is a Centralized Exchange (CEX)? [Електронний ресурс]. – Режим доступу: https://surl.li/sslyvt

7. Decentralized Applications (DApps) / Investopedia [Електронний ресурс]. – Режим доступу: https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp

8. Bitfinex Suspects It’s Being Attacked Again [Електронний ресурс]. – Режим доступу: https://www.bloomberg.com/news/articles/2018-06-05/crypto-exchange-bitfinex-suspects-it-s-being-attacked-again

9. Exploring the DAO Hack: Lessons Learned for Web3 Security [Електронний ресурс]. – Режим доступу: https://securrtech.medium.com/exploring-the-dao-hack-lessons-learned-for-web3-security-08d23984af79

10. Youbit Bitcoin exchange quits operation after 2 hacks in 8 months // HackRead, 2017 [Електронний ресурс]. – Режим доступу: https://hackread.com/youbit-bitcoin-exchange-quits-operation-after-2-hacks/

11. DDoS Attacks on Crypto Exchanges in 2021 [Електронний ресурс]. – Режим доступу: https://stormwall.network/resources/blog/ddos-attacks-impact-on-crypto-exchange-2021stormwall.network

12. Державна служба спеціального зв'язку та захисту інформації України. Аналітична довідка щодо кіберінцидентів, зафіксованих у 2023 році [Електронний ресурс]. – Режим доступу: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006

13. Why the KYC Procedure is Beneficial for Both Exchanges and Users [Електронний ресурс]. – Режим доступу: https://podolyanin.com.ua/advertisement/75252/

14. How HTTPS Works [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/learning/ssl/what-is-https/

15. Babko, A. Role-based Access Control vs Attribute-based Access Control: Which to Choose [Електронний ресурс]. – Режим доступу: https://www.syteca.com/en/blog/rbac-vs-abac

16. Міллер, Дж. IDS vs IPS vs SIEM: What You Should Know [Електронний ресурс]. – Режим доступу: https://www.bitlyft.com/resources/ids-vs-ips-vs-siem

17. Coinbase. Coinbase Custody attains its SOC 1 and SOC 2 reports [Електронний ресурс]. – Режим доступу: https://www.coinbase.com/blog/in-another-first-coinbase-custody-attains-its-soc-1-and-soc-2-reports

18. Binance. Binance secures SOC 2 Type 2 and SOC 1 Type 1 certifications [Електронний ресурс]. – Режим доступу: https://www.binance.com/en/blog/all/strengthening-security-and-transparency-binance-secures-soc-2-type-2-and-soc-1-type-1-certifications-1685407653774568727

19. Україна. Закон «Про віртуальні активи» від 17 лютого 2022 р. № 2074-IX [Електронний ресурс] // Верховна Рада України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2074-20#Text

20. Bitcoin Improvement Proposal BIP-0039: Mnemonic code for generating deterministic keys [Електронний ресурс]. – Режим доступу: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

21. Forbes. Fortify Your Digital Wealth: Expert Tips for Safe Seed Phrase Storage // Forbes Digital Assets, 30.01.2024 [Електронний ресурс]. – Режим доступу: https://www.forbes.com/sites/digital-assets/2024/01/30/fortify-your-digital-wealth-expert-tips-for-safe-seed-phrase-storage

22. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – 3rd ed. – Wiley, 2020. – 1184 p.

23. MITRE Corporation. Using UEBA to Detect Insider Threats and Anomalies [Електронний ресурс]. – Режим доступу: https://www.mitre.org/publications/technical-papers/ueba-insider-threat-detection

24. Ledger. Seed Phrase Storage [Електронний ресурс]. – Режим доступу: https://shop.ledger.com/pages/seed-phrase-storage

25. Patrick Alpha. Top 9 Cryptocurrency Hardware Wallets for 2025 [Електронний ресурс] // Medium, 2025. – Режим доступу: https://patrickalphac.medium.com/top-9-cryptocurrency-hardware-wallets-for-2025-security-researcher-review-9fcb16d771e0

# ДОДАТОК А

## Лістинг програмного модуля

**main()**

```
from utils.shamir_tools import split_secret, recover_secret
from utils.storage import save_to_file, read_from_file
from utils.qr_tools import generate_qr, read_qr
from utils.telegram_tools import send_qr_to_telegram
def create_wallet(seed_phrase):
    print("Розділяємо seed-фразу...")
    parts = split_secret(seed_phrase)
    part_A, part_B, part_C = parts
    print("\n Зберігаємо частини...")
    save_to_file(part_A, "part_A.txt")
    generate_qr(part_B, "part_B_qr.png")
    send_qr_to_telegram("part_B_qr.png")
    print("\n Частина C (запишіть на папір, не зберігається автоматично):")
    print("", part_C)
    print("\n Гаманець створено:")
    print(" - Частина A збережена у файлі part_A.txt")
    print(" - Частина B збережена як QR у файлі part_B_qr.png")
    print(" - Частина C виведена в консоль для ручного запису")
def recover_wallet():
    print("Відновлення seed-фрази")
    part1 = input("Введіть першу частину (з файла або з паперу): ").strip()
    part2 = input("Введіть другу частину (з QR або файла): ").strip()
    shares = [part1, part2]
    try:
        seed = recover_secret(shares)
        print("\n🔑Відновлена seed-фраза:")
        print( seed)
    except Exception:
        pass
    seed_for_display = input()
    print(seed_for_display)
if __name__ == "__main__":
    print(" CryptoColdShare — головне меню")
    print("1. Створити гаманець")
    print("2. Відновити гаманець")
    choice = input("> ")
    if coice == "1":
```

```
  seed = input("Введіть seed-фразу для збереження:\n> ")
      create_wallet(seed)
   elif choice == "2":
      recover_wallet()
   else:
      print(" Невідома опція")
```

**shamir_tools.py**

```
import random
# Велике просте число для поля
PRIME = 2 ** 127 - 1
def eval_polynomial(coeffs, x, prime=PRIME):
   """Обчислення значення полінома в точці x по модулю prime."""
   result = 0
   for coefficient in reversed(coeffs):
      result = (result * x + coefficient) % prime
   return result
def split_secret(seed_phrase, num_parts=3, threshold=2):
   """Розбиття seed-фрази на частини за схемою Shamir (2 з 3)."""
   secret_int = int.from_bytes(seed_phrase.encode(), 'utf-8')
   coeffs = [secret_int] + [random.SystemRandom().randint(0, PRIME - 1) for _
in range(threshold - 1)]
   shares = []
   for i in range(1, num_parts + 1):
      x = i
      y = eval_polynomial(coeffs, x)
      shares.append(f"{x}-{y}")
   return shares
def lagrange_interpolate(x, x_s, y_s, prime=PRIME):
   """Інтерполяція Лагранжа для відновлення значення в точці x."""
   total = 0
   for i in range(len(x_s)):
      xi, yi = x_s[i], y_s[i]
      prod = yi
      for j in range(len(x_s)):
         if i != j:
```

```
                xj = x_s[j]
                inv = pow(xi - xj, -1, prime)  # Обернене за модулем
                prod *= (x - xj) * inv
                prod %= prime
            total += prod
            total %= prime
        return total
    def recover_secret(shares):
        """Відновлення seed-фрази з частин."""
        points = [(int(s.split("-")[0]), int(s.split("-")[1])) for s in shares]
        x_s, y_s = zip(*points)
        secret_int = int(lagrange_interpolate(0, x_s, y_s, PRIME))
        secret_bytes = secret_int.to_bytes((secret_int.bit_length() + 7) // 8, 'big')
        try:
            return secret_bytes.decode('utf-8')
        except UnicodeDecodeError:
            # Якщо декодування не вдається - повернути hex для діагностики
    return secret_bytes.hex()
```

**recover_secret(shares)**

```
    def recover_secret(shares):
        points = [(int(s.split("-")[0]), int(s.split("-")[1])) for s in shares]
        x_s, y_s = zip(*points)
        secret_int = int(lagrange_interpolate(0, x_s, y_s, PRIME))
        secret_bytes = secret_int.to_bytes((secret_int.bit_length() + 7) // 8, 'big')
return secret_bytes.hex()
```

**create_wallet()**

```
    from mnemonic import Mnemonic
    from utils.shamir_tools import split_secret
    from utils.qr_tools import generate_qr
    from utils.storage import save_to_file
    from utils.telegram_bot import send_qr_to_telegram
    def create_wallet():
```

**Продовження додатку А**

```
    mnemo = Mnemonic("english")
    seed_phrase = mnemo.generate(strength=128)
    print("\n Seed-фраза згенерована!")

    shares = split_secret(seed_phrase, 3, 2)
    save_to_file(shares[0], "data/part_A.txt")
    print(" Частина A збережена локально у файл data/part_A.txt")
    generate_qr(shares[1], "data/part_B_qr.png")
    send_qr_to_telegram("data/part_B_qr.png")
    print("Частина B відправлена у Telegram як QR-код")
    print("\n Частина C (запишіть на папері):")
    print("-------------------------------------------------")
    print(shares[2])
    print("-------------------------------------------------")
    print("\n    Гаманець створено й розподілено на 3 частини.")
if __name__ == "__main__":
    create_wallet()
```

# ДОДАТОК Б
# СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

## Тези наукових конференцій

Бондаренко Я. Безпека криптовалютних бірж та холодних гаманців: розробка плану захисту / Яна Бондаренко, Яніна Шестак / VIII Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)” 11 квітня 2025 року, Київ, Україна. С 157-160.