

Секція 1

**ДОСЛІДЖЕННЯ КІБЕРРИЗИКІВ ТА РОЗРОБЛЕННЯ СТРАТЕГІЙ
ЗАХИСТУ КРИПТОВАЛЮТНИХ ТРЕЙДЕРІВ З УРАХУВАННЯМ
РЕГУЛЯТОРНИХ ВИМОГ**

Пархоменко Є. О.

Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Морозова О. І.

Актуальність. Сьогодні захист криптовалютних інвесторів та трейдерів від кібер-ризиків є важливим аспектом безпеки у фінансовому та цифровому просторі. З розвитком ринку криптовалют зросла кількість кіберзагроз, таких як фішингові атаки, шкідливе програмне забезпечення та атаки на криптовалютні біржі. Ці ризики не тільки створюють загрозу втрати активів для інвесторів, але й порушують регуляторні вимоги, встановлені для безпеки ринку, такі як «Anti Money Laundering» (AML, «боротьба з відмиванням грошей») та «Know Your Customer» (KYC, «знай свого клієнта»). Тому існує нагальна потреба у застосуванні стратегій хеджування, які б гарантували безпеку активів інвесторів та відповідали останнім регуляторним стандартам [1, 2].

Мета роботи. Метою цієї роботи є аналіз основних кіберризиків, з якими стикаються криптовалютні трейдери та розробка комплексної стратегії захисту, що відповідає регуляторним вимогам та забезпечує безпечне середовище для трейдерів.

Основні положення. Розглянемо основні кіберризики, пов'язані з криптовалютними трейдерами та біржами. Фішинг – метод, спрямований на отримання доступу до конфіденційної інформації інвесторів через підроблені веб-сайти та повідомлення. Шкідливе програмне забезпечення – комп'ютерні програми, які крадуть особисту інформацію або фінансові активи. 51 атака – ситуація, коли одна група або невелика кількість користувачів може взяти під контроль мережу блокчейн і модифікувати дані блокчейну. Крадіжка біржових активів – коли інвестори втрачають свої активи через злом криптовалютних бірж [2, 3].

Також проаналізовано вимоги регуляторів щодо підвищення безпеки. Принципи KYC – вимоги до інвесторів підтверджувати свою особу для запобігання шахрайству. AML – стандарти боротьби з відмиванням грошей, які зменшують можливість незаконного використання криптовалют. Захист персональних даних – дотримання законодавства про захист персональних

даних, зокрема вимог General Data Protection Regulation (GDPR, загальний регламент про захист даних).

Ключовим елементом цього дослідження є розроблення особливо ефективних стратегій захисту. Використання апаратних гаманців для безпечного зберігання криптовалют. Багаторівнева аутентифікація – додатковий рівень захисту облікового запису. Регулярний аудит бірж і торгових платформ для виявлення та усунення можливих вразливостей.

Висновки. У дослідженні було проаналізовано основні кіберризики в секторі торгівлі криптовалютами та розроблено стратегію захисту на основі регуляторних вимог. Проаналізовано основні типи атак, що загрожують безпеці трейдерів, та методи захисту для мінімізації цих ризиків. Було виявлено, що використання комплексних підходів до безпеки, таких як апаратні гаманці та багаторівнева автентифікація, є важливими для захисту активів. Впровадження цих рекомендацій сприятиме підвищенню безпеки криптовалютного ринку та зміцненню довіри інвесторів.

Список літератури

1. Researching cyber risks. *StackExchange*. URL – <https://security.stackexchange.com/search?q=Researching+cyber+risks> (дата звернення: 09.11.2024).
2. Developing a Crypto Trading Strategy: A Beginner's Guide. *Openware*. URL – <https://www.openware.com/news/articles/developing-a-crypto-trading-strategy-a-beginners-guide> (дата звернення: 10.11.2024).
3. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. *Semantic scholar*. URL – <https://www.semanticscholar.org/paper/There%27s-No-Free-Lunch%2C-Even-Using-Bitcoin%3A-Tracking-Vasek-Moore/c102f5dbb4e3bbcca3d36583fde14caf2212931> (дата звернення: 10.11.2024).

Відомості про авторів

Пархоменко Євген Олександрович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.parkhomenko@student.csn.khai.edu
 Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, o.morozova@khai.edu