Криптозлочинність: тенденції, методи та виклики для правового регулювання цифрових активів

Костянтин Кривенко
адвокат, радник,
керівник практики кримінального права
АО «ЮФ «Ілляшев та Партнери»,
аспірант 3-го року підготовки,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: KryvenkoKO@krok.edu.ua,
ORCID: 0009-0006-1327-757X

Автором зроблено аналітичний огляд ключових тенденцій криптозлочинності за результатами аналізу «The 2025 Crypto Crime Report (Chainalysis)» [1], що охоплює події 2024 року. Висвітлено основні види злочинів, їхню динаміку, типові методи та інструменти злочинців. Особливу увагу приділено питанням відмивання коштів через стейблкоїни, використанню штучного інтелекту у шахрайських схемах та ролі державних органів у боротьбі з кіберзлочинністю. Зроблено висновки щодо пріоритетних напрямів удосконалення правового регулювання обігу віртуальних активів.

Загальні тенденції

Минулий рік позначився не лише зростанням масштабів використання криптовалют у легальному секторі, а й поглибленням структурної складності злочинних схем. За оцінками Chainalysis, частка незаконних транзакцій у загальному обсязі криптоопераций залишається відносно незначною — менше 0,5%, однак загальна сума таких операцій перевищує 40-50 млрд доларів США. Це свідчить про перехід від дрібних індивідуальних правопорушень до системних і професійно організованих схем.

Криптозлочинність сьогодні — це багаторівневе явище, у якому поєднуються елементи фінансових махінацій, кіберзлочинів і традиційних злочинів економічного характеру. На відміну від попередніх років, 2024 рік засвідчив не стільки кількісне зростання інцидентів, скільки якісне вдосконалення методів і активне залучення технологічних інструментів, зокрема штучного інтелекту.

У сучасній науковій літературі дедалі частіше звертають увагу на те, що криптовалюти виступають каталізатором для нових форм кіберзлочинності, трансформуючи традиційні схеми шахрайств і відмивання через додаткову анонімність, швидкість і децентралізованість транзакцій [2].

Також у праці «An Anatomy of Crypto-Enabled Cybercrimes» підкреслюється, що організовані угруповання, які займаються криптокіберзлочинами (зокрема ransomware), фактично функціонують як корпорації: вони застосовують стратегії управління репутацією, диверсифікацію бізнес-моделей і контроль ризиків [3]. Цей підхід «як фірма» дозволяє їм витримувати законодавчий тиск, змінювати структуру діяльності, адаптувати технології і вкладати ресурси в інфраструктуру злочинного бізнесу.

Основні категорії криптозлочинів

У звіті Chainalysis [1] виокремлено п’ять основних категорій злочинів, що формують ядро сучасної криптозлочинності:

• ***крадіжки та злами (hacks, exploits)*** Протягом 2024 року обсяг викрадених коштів сягнув приблизно 2,2 млрд доларів США, що на 21% більше, ніж у 2023 році. Понад половину цих втрат (61%) пов’язано з діяльністю хакерських угруповань, афілійованих із Північною Кореєю. Основні методи — експлойти смарт-контрактів, компрометація приватних ключів, атаки на DeFi-мости та централізовані біржі.

• ***шахрайство (scams)*** Прибутки злочинців від різних форм шахрайства оцінюються у 10–12 млрд доларів США. Найбільш поширеною моделлю став так званий pig butchering — створення тривалих довірчих відносин із жертвою (часто у романтичному чи бізнес-контексті) для подальшого виманювання коштів. Також зафіксовано зростання кількості інвестиційних схем з обіцянками надвисоких прибутків та фішингових атак.

• ***вимагання (ransomware)*** Загальні суми викупів, сплачених у криптовалютах, досягли рекордних рівнів, навіть попри зменшення кількості атак. Це пояснюється концентрацією ринку у руках небагатьох високопрофесійних угруповань, які діють із використанням методів анонімізації та децентралізованих платіжних каналів.

• ***відмивання доходів та ухилення від санкцій*** Понад 60% нелегальних транзакцій здійснюються через стейблкоїни, що стали універсальним інструментом для приховування походження коштів. Відмивання проводиться через міксери, децентралізовані біржі (DEX) та транзитні гаманці у юрисдикціях із низьким рівнем контролю.

• ***нелегальна торгівля у даркнеті*** Незважаючи на закриття низки великих платформ, обсяги продажів наркотиків і заборонених товарів через криптовалюту зросли приблизно на 19%. Основними валютами залишаються Bitcoin і Monero, останній завдяки своїй підвищеній конфіденційності.

Поряд із технічними експлойтами, важливу роль відіграють соціальна інженерія та психологічний вплив. Використання генеративного ШІ дало змогу злочинцям створювати персоналізовані повідомлення, аватари та навіть голосові deepfake-дзвінки. Це значно ускладнює виявлення шахрайства.

DeFi-сектор залишається зоною підвищеного ризику через відкритість коду і відсутність централізованого управління. Натомість централізовані біржі (CEX) частіше стають проміжними ланками для відмивання та обміну «злочинних» активів на стейблкоїни.

Сучасна криптозлочинність виходить за межі національних юрисдикцій, що робить традиційні інструменти кримінального переслідування малоефективними. Основними проблемами є:

• відсутність уніфікованих стандартів комплаєнсу та блокчейн-моніторингу;

• складність ідентифікації кінцевих бенефіціарів транзакцій;

• недостатня міжнародна координація між фінансовими розвідками та пра-

воохоронними органами.

Chainalysis рекомендує впровадження ризик-орієнтованих моделей моніторингу, розвиток аналітики блокчейн-транзакцій та створення єдиних процедур замороження цифрових активів.

Для України та країн ЄС особливо актуальною є гармонізація правових підходів до обігу віртуальних активів, узгодження визначень понять «віртуальний актив», «постачальник послуг у сфері віртуальних активів (VASP)» та механізмів відповідальності за порушення у сфері AML/KYC.

Висновки

Криптозлочинність набуває ознак високотехнологічної, транснаціональної і напівавтоматизованої діяльності. Штучний інтелект, DeFi-інфраструктура та стейблкоїни водночас відкривають нові можливості для бізнесу і створюють безпрецедентні ризики для безпеки фінансової системи.

Правове регулювання має бути технологічно нейтральним, проте здатним оперативно реагувати на інновації. У цьому контексті ключовим завданням є створення системи міжнародної взаємодії та обміну аналітичними даними, що забезпечить прозорість руху цифрових активів і підвищить ефективність кримінального переслідування.

Ключові слова: віртуальні активи, криптоактиви, криптовалюта, цифрові активи, правове регулювання обігу віртуальних активів, цифрова економіка.

Список використаних джерел

1. The 2025 Crypto Crime Report: The rising role of cryptocurrency in all forms of crime and how its transparency is creating unique opportunities for investigation. Chainalysis (2025) URL: https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf [дата посилання 28.11.2025].

2. Trozze, A., Kamps, J., Akartuna, E.A. et al. Cryptocurrencies and future financial crime. Crime Sci 11, 1 (2022). URL: https://doi.org/10.1186/s40163-021-00163-8 [дата посилання 28.11.2025].

3. Will Cong, Campbell Harvey, Daniel Rabetti, Zong-Yu Wu (2025) An Anatomy of Crypto-Enabled Cybercrimes. Management Science 71(4):3622-3633. URL: https://doi.org/10.1287/mnsc.2023.03691 [дата посилання 28.11.2025].