УДК 343.4:[342.7:004]](477+100)
DOI: 10.21564/2414-990X.173.361496

Способи посягання на криптовласність: основні види та кваліфікація

Іван Едуардович Щеглаков*
Національний юридичний університет імені Ярослава Мудрого, Харків, Україна
**e-mail: shived1@ukr.net*

Анотація
Стрімке зростання капіталізації ринку криптоактивів зумовило збільшення кількості кримінально протиправних посягань на криптовласність. Технологічна складність та цифрова природа криптоактивів породжують нові способи їх протиправного заволодіння, що створює потребу в науковій систематизації таких посягань і формуванні єдиних підходів до їх кримінально-правової кваліфікації. Метою статті є здійснення класифікації основних способів викрадення криптоактивів та визначення на основі аналізу механізму їх вчинення особливостей кримінально-правової кваліфікації цих діянь за кримінальним законодавством України. Використано діалектичний, формально-юридичний, системно-структурний, порівняльно-правовий і соціологічний методи. Запропоновано поділ способів посягання на криптовласність на дві групи: традиційні (насильницькі викрадення, обманні заволодіння, привласнення, розтрата або заволодіння шляхом зловживання службовим становищем) та нетрадиційні (використання шпигунського програмного забезпечення, підміна платіжних реквізитів, застосування підроблених токенів, експлуатація вразливостей смарт-контрактів). У випадках застосування технічних засобів втручання в роботу інформаційних систем дії винного потребують додаткової кваліфікації за статтями розділу XVI Кримінального кодексу України.

Ключові слова: криптоактиви; криптовалюта; кримінальні правопорушення проти власності; шахрайство; крадіжка; блокчейн.

Methods of Encroachment on Cryptoproperty: Main Types and Qualification

Ivan E. Shchehlakov*
Yaroslav Mudryi National Law University, Kharkiv, Ukraine
**e-mail: shived1@ukr.net*

Abstract

The rapid growth in the capitalisation of the cryptoasset market has led to an increase in the number of criminal encroachments on cryptoproperty. The technological complexity and digital nature of cryptoassets give rise to new methods of their unlawful acquisition, which creates a need for the scientific systematisation of such encroachments and the formation of unified approaches to their criminal-law qualification. The aim of the article is to classify the principal methods of stealing cryptoassets and, based on the analysis of the mechanism by which they are committed, to determine the specific features of the criminal-law qualification of such acts under the criminal legislation of Ukraine. The dialectical, formal-legal, system-structural, comparative-legal, and sociological methods have been employed. It is proposed to divide the methods of encroachment on cryptoproperty into two groups: traditional (violent seizures, fraudulent acquisitions, misappropriation, embezzlement, or seizure through the abuse of office) and non-traditional (the use of spyware, substitution of payment details, the use of counterfeit tokens, and exploitation of vulnerabilities in smart contracts). In cases involving the use of technical means of interference in the operation of information systems, the perpetrator's actions require additional qualification under the articles of Chapter XVI of the Criminal Code of Ukraine.

Keywords: cryptoassets; cryptocurrency; criminal offenses against property; fraud; theft; blockchain.

Вступ

Минулий, 2025, рік ознаменувався безпрецедентним зростанням ринку криптоактивів. За даними Coingecko, сукупна ринкова капіталізація криптоактивів у третьому кварталі 2025 р. досягла історичного максимуму в чотири трильйони доларів США [1]. Цей показник перевищує капіталізацію всього світового ринку срібла, що, у свою чергу, свідчить про те, що станом на сьогодні криптоактиви є не просто спекулятивним інструментом, а виконують функції засобу накопичення, інвестиційного активу, а в деяких країнах (наприклад, у Сальвадорі) – й функцію платіжного засобу.

Криптоактиви фактично стали в один ряд із традиційними матеріальними цінностями: нерухомістю, банківськими металами та фіатними грошима. Проте діалектика технологічного прогресу має і зворотний бік: стрімке зростання вартості активів неминуче виступає каталізатором злочинної активності.

Висока ліквідність, псевдоанонімність транзакцій та транскордонний характер обігу роблять криптоактиви мішенню для злочинців. Новизна явища криптоактивів, а також його технічна складність зумовлюють швидку еволюцію способів викрадення цих активів. Спектр кримінально протиправних посягань у цій сфері набув надзвичайного різноманіття: від класичних способів заволодіння (шляхом застосування насильства або обману) до високотехнологічних (використання шпигунського програмного забезпечення, зломи тощо).

Така різноманітність способів вчинення кримінальних правопорушень, спрямованих на викрадення криптоактивів, створює нагальну потребу в науковій систематизації видів кримінально протиправних посягань проти власності на криптоактиви (криптовласність) задля розмежування складів кримінальних правопорушень проти власності.

Огляд літератури

У сучасній кримінально-правовій доктрині існують різні підходи до розуміння змісту та обсягу предмета кримінальних правопорушень проти власності, зокрема щодо можливості віднесення до предметів цих правопорушень неуречевленого майна. Тривалий час у вітчизняній науці панівною є думка, що у розд. VI Особливої частини Кримінального кодексу України (далі – КК) термін «майно» вжито у значенні цивільно-правового визначення «річ», тобто охоплює лише предмети матеріального світу [2, с. 350].

Утім такий погляд дедалі частіше стає предметом дискусій, адже, як зазначає А. О. Антонюк, еволюція власності та її розвиток у напрямі «неуречевленості» зумовлюють перегляд усталених підходів [3, с. 113]. Л. М. Демидова обстоює думку про те, що предметом кримінальних правопорушень на рівні з тілесними речами є й речі безтілесні, які можуть бути введені в майновий оборот та мати грошову вартість [4, с. 106]. Ю. А. Дорохіна пропонує переглянути поняття власності у кримінальному праві України шляхом переходу до широкого його розуміння, яке, зокрема, включає в себе і криптовалюту [5, с. 149, 170].

Із такими доводами важко не погодитись: цифровізація економіки, виникнення нових об'єктів права власності у вигляді криптоактивів, зміна законодавства (зокрема в частині введення в обіг поняття «цифрова річ») лише зумовлює потребу в переосмисленні та осучасненні розуміння предмета кримінальних правопорушень проти власності. Цю тезу також підкріплено тим, що криптоактиви є об'єктом переважно майнових правовідносин і, володіючи криптоактивами, суб'єкт правовідносин ставиться до них як до свого власного майна. Намагаючись незаконно заволодіти криптоактивами, зловмисник передусім має за мету обернути їх на свою користь, протиправно збагатитися. Тож протиправні посягання на криптоактиви мають розглядатись як посягання проти власності.

У вітчизняній науковій літературі вже існує значна кількість праць, у яких наголошено на можливості криптоактивів виступати предметом кримінальних правопорушень проти власності. Так, наприклад, О. В. Кришевич та О. І. Рощина зауважують, що криптовалюта може бути предметом крадіжки, вимагання та шахрайства, одночасно підкреслюючи, що такі кримінальні

правопорушення мають свої особливості, зумовлені природою криптовалюти [6, с. 171–172].

М. О. Думчиков акцентує увагу на тому, що домінуючим способом заволодіння криптоактивами є шахрайство, основними видами якого є цільовий фішинг, шахрайство з купівлею та обміном віртуальних активів, а також інвестування у фіктивні віртуальні активи [7, с. 162].

В. В. Козій також наголошує на тому, що криптовалюта може бути предметом крадіжки, привласнення (заволодіння) та шахрайства [8, с. 37].

Отже, попри консенсус значної кількості дослідників щодо необхідності кримінально-правової охорони криптоактивів, у вітчизняній доктрині досі відсутні ґрунтовні наукові розробки, присвячені як видам посягань на криптоактиви, так і систематизації способів протиправного заволодіння ними. Більшість праць зосереджені на загальному питанні: «чи є криптоактиви (віртуальні активи, криптовалюта) майном у розумінні КК?», залишаючи поза увагою способи їх викрадення. Водночас розуміння конкретного алгоритму вчинення цих кримінальних правопорушень є критично необхідним для правильної кваліфікації діянь та їх відмежування від суміжних складів кримінальних правопорушень.

Матеріали та методи

Під час написання статті використовувались як загальнонаукові, так і спеціально-юридичні методи, що зумовлено міждисциплінарним характером проблематики, яка перебуває на стику кримінального права та інформаційних технологій. Вибір методології зумовлений необхідністю одночасного аналізу як юридичних явищ, так і технологічних особливостей предмета посягання – криптоактивів, без розуміння природи яких неможлива правильна кримінально-правова оцінка способу вчинення відповідних діянь.

Загальнометодологічну основу становив діалектичний метод, що дав змогу розглянути способи посягання на криптовласність у їх розвитку та взаємозв'язку з технологічними змінами, що відбуваються у криптосфері.

Формально-юридичний метод використовувався для з'ясування змісту положень законодавства, тлумачення ознак конкретних складів кримінальних правопорушень, а також для аналізу правових дефініцій.

Системно-структурний метод став основним інструментом класифікації способів посягання на криптовласність. Завдяки його застосуванню вдалося виокремити дві великі групи способів вчинення таких посягань – традиційні та нетрадиційні, а також встановити внутрішню структуру кожної з груп.

Порівняльно-правовий метод використано для зіставлення підходів вітчизняної та зарубіжної доктрини й практики до кримінально-правової оцінки посягань на криптоактиви. Особливу увагу приділено англомовній науковій літературі, що зумовлено первинною появою більшості новітніх кримінально протиправних схем саме в англомовних юрисдикціях.

Соціологічний метод у формі аналізу матеріалів правозастосовної практики використано для виявлення типових моделей поведінки суб'єктів кримінальних правопорушень.

Написання статті включало кілька етапів: опрацювання вітчизняної та зарубіжної наукової правничої літератури; аналіз нормативно-правової бази; формування емпіричної бази дослідження із судових рішень, матеріалів резонансних зарубіжних кримінальних проваджень та звітів спеціалізованих компаній у сфері блокчейн-аналітики; систематизація та класифікація виявлених способів посягання; формулювання пропозицій щодо їх кримінально-правової кваліфікації.

Результати та обговорення

Заволодіння криптоактивами відбувається широким колом способів, через що саме спосіб вчинення кримінального правопорушення є тією ознакою, за якою слід розмежовувати посягання на криптовласність.

Криптоактиви є одним із видів майна, якому притаманні такі специфічні ознаки, як існування виключно в цифровому середовищі, а також функціонування та зберігання на основі технології розподіленого реєстру чи подібної до неї технології [9, с. 238]. На основі цього способи посягань проти власності, предметом яких є криптоактиви, можна поділити на традиційні (способи викрадення (заволодіння), притаманні кримінальним правопорушенням, предметом яких може бути будь-яке майно) та нетрадиційні (специфічні способи викрадення (заволодіння), зумовлені цифровою природою активів). Більшість із них відомі українській правозастосовній практиці, однак деякі зустрічалися до цього часу тільки в інших країнах, проте, імовірно, незабаром з'являться й в Україні.

І. Традиційні способи посягання

Під традиційними способами пропонується розуміти форми протиправного посягання, які характерні для більшості кримінальних правопорушень проти власності. Здійснюючи викрадення криптоактивів або заволодіння ними у традиційний спосіб, суб'єкт кримінального правопорушення досягає своєї протиправної мети, як правило, шляхом впливу на потерпілого, наприклад, застосовуючи до нього насильство, змушуючи передати криптоактиви,

або ж використовуючи слабкості потерпілого для введення його в оману щодо вигідності тієї чи іншої транзакції. При цьому суб'єкт кримінального правопорушення не використовує (або використовує мінімально) специфічний технічний інструментарій чи вразливості програмного забезпечення. У таких випадках цифрова природа активу та технологічні особливості його функціонування (блокчейн, децентралізація) або взагалі не мають ніякого значення для зловмисника, або ж відіграють лише другорядну роль. Визначальним для досягнення злочинного результату має не подолання системи захисту, втручання в роботу електронних обчислювальних машин, використання вразливостей програмного забезпечення, а подолання чи викривлення волі потерпілого або ж використання наявних повноважень щодо криптоактивів. Спосіб викрадення (заволодіння) у цьому разі є універсальним та ідентичним до механізму викрадення будь-якого іншого рухомого майна або грошових коштів. Технологічний складник при цьому є лише середовищем обігу активів, утім аж ніяк не сприяє суб'єкту у вчиненні кримінального правопорушення.

До найбільш поширених традиційних способів посягань на відносини власності на криптоактиви слід віднести такі.

1. Насильницькі викрадення

Викрадення криптоактивів із застосуванням насильства може включати як фізичне, так і психічне насильство. Такий спосіб викрадення є найбільш суспільно небезпечним, адже об'єктом посягання в такому випадку є не лише криптоактиви, а й життя, здоров'я та тілесна недоторканність особи. В англомовних країнах такий спосіб викрадення має назву «$5 Wrench Attack» («Атака з гайковим ключем за 5 доларів»). Така назва підкреслює примітивність дій зловмисника: не бажаючи розбиратися в технічних деталях, злочинець просто використовує фізичну силу або залякування для обернення криптоактивів на свою користь.

Британські дослідники Marilyne Ordekian, Gilberto Atondo-Siu, Alice Hutchings та Marie Vasek пропонують визначати «атаку з гайковим ключем» як фізичне переслідування власників криптовалюти з метою незаконного заволодіння їх криптовалютою за допомогою фізичної сили або погрози застосування сили чи заподіяння шкоди [10, с. 24:4].

Компанія TRM Labs, яка надає послуги блокчейн-аналітики для виявлення кримінальних правопорушень, на своєму вебсайті наводить найбільш відомі приклади «атак з гайковим ключем». Так, одним із перших зафіксованих випадків подібної атаки є інцидент, що стався з криптотрейдером Danny Aston: група з чотирьох озброєних осіб здійснила проникнення до приват-

ного будинку потерпілого. Застосувавши фізичне насильство та обмеживши свободу дівчини криптотрейдера, нападники під загрозою застосування вогнепальної зброї змусили трейдера здійснити транзакцію з переказу Bitcoin на підконтрольні їм криптогаманці.

Іншим прикладом є інцидент у гуртожитку Кентерберійського університету, де в 2021 р. один із студентів був затриманий групою з восьми чоловіків, які через погрозу ножем змусили його переказати Bitcoin у сумі, що була еквівалентна 6000 фунтів стерлінгів [11].

Із аналізу вітчизняної правозастосовної практики вбачається, що подібні випадки насильницького заволодіння трапляються і в Україні.

Так, вироком Обухівського районного суду Київської області від 06.12.2022 р. у справі № 761/31532/21 Особу_8 та Особу_9 визнано винуватими у вчиненні злочину, передбаченого ч. 4 ст. 187 КК. При цьому судом встановлено, що Особа_8 помітив серед програм на телефоні потерпілого програму для криптовалют «Binance», після чого Особа_8 у співучасті з Особою_9 наносили тілесні ушкодження ножем у ногу потерпілого, погрожували пістолетом, внаслідок чого потерпілий повідомив всі необхідні паролі, завдяки чому Особа_8 та Особа_9 заволоділи криптовалютою, а саме 2 Ethereum (ETH), та 5436,001 Stellar (XLM) [12].

За даними Київської міської прокуратури, чотирьом особам було вручено повідомлення про підозру у вчиненні вимагання, яке виявилося в тому, що ці особи, представляючись правоохоронцями, погрожували криптобізнесмену кримінальною відповідальністю за вигаданими обвинуваченнями у державній зраді, внаслідок чого змусили потерпілого перерахувати криптовалюту на суму майже 10 млн гривень на їхній криптогаманець [13].

Так, насильницьким викраденням криптоактивів притаманні такі ознаки:

– наявність двох об'єктів посягання: основним об'єктом виступають відносини власності на криптоактиви, а додатковим об'єктом – особисті немайнові блага потерпілого (життя, здоров'я, особиста свобода, тілесна недоторканність тощо);
– застосування насильства: основним способом, за допомогою якого суб'єкт кримінального правопорушення реалізує свою кримінально протиправну мету, є насильство, яке може бути як фізичним (у вигляді завдання фізичної шкоди потерпілому), так і психічним (погрози фізичної розправи, обмеження прав, знищення майна тощо). Насильство може використовуватись як для безпосереднього отримання винним доступу до криптогаманця потерпілого, так і для пригнічення волі потерпілого для самостійного здійснення ним передачі криптоактивів.

Залежно від характеру насильства (небезпечності насильства для життя та здоров'я в момент заподіяння або погрози його заподіяння), а також темпоральної спрямованості такого насильства (чи має винний намір заволодіти криптоактивами негайно, чи висуває вимогу щодо їхньої передачі в майбутньому) викрадення криптоактивів у формі «атаки з гайковим ключем за 5 доларів» мають кваліфікуватись як насильницький грабіж (ч. 2 ст. 186 КК), розбій (ст. 187 КК) або вимагання (ст. 189 КК).

2. Обманні заволодіння

Другу велику групу традиційних способів незаконного заволодіння криптоактивами становлять діяння, механізм яких ґрунтується на інтелектуальному впливі на свідомість потерпілого. На відміну від насильницьких кримінальних правопорушень, заволодіння криптоактивами тут відбувається ззовні добровільно – власник самостійно ініціює транзакцію та передає активи зловмиснику.

Так, наприклад, вироком Оболонського районного суду міста Києва від 10.12.2024 р. у справі № 756/12186/24 встановлено, що Особа_5 створив телеграм-канал, зареєстрований під нікнеймом, який дублював один із відомих сервісів обміну валют, за винятком умисного неправильного зазначення декількох латинських літер, що вводило в оману потерпілого щодо дійсного суб'єкта надання таких послуг, у якому розмістив завідомо неправдиве оголошення про те, що у вказаному телеграм-каналі можливо домовитись про безпечний обмін криптовалюти. Через вказаний телеграм-канал до Особи_5 звернувся потерпілий із пропозицією обміну криптоактиву USDT у сумі 21398. Отримавши 21 398 USDT, винний жодного обміну на фіатну валюту не здійснив [14].

У справі № 513/1179/24 Саратським районним судом Одеської області Особу_7 визнано винним у вчиненні шахрайства, у ході якого винний запевнив потерпілого в тому, що може надати йому допомогу у сфері заробітку грошових коштів у мережі «Інтернет2, після чого потерпілий погодився оплатити таку допомогу в USDT, проте після отримання криптоактивів винний жодних зобов'язань не виконав [15].

Однією з поширених схем обманного заволодіння криптоактивами є «Шахрайський трикутник» (англ. «Triangulation Fraud»), сутність якої полягає в «синхронізації» зловмисником двох незалежних правочинів, внаслідок чого потерпілий, будучи введеним в оману, виконує грошові зобов'язання зловмисника перед іншою особою, фактично сплачуючи вартість криптоактивів, отримувачем яких стає злочинець. Наприклад, зловмисник розміщує оголошення про продаж неіснуючого товару і після появи реального покупця

паралельно ініціює на P2P-платформі (або криптобіржі) ордер на купівлю криптоактивів у трейдера на аналогічну суму. Отримавши від трейдера банківські реквізити, зловмисник передає їх покупцю товару під виглядом власних. У результаті покупець переказує грошові кошти на рахунок трейдера, а той, фіксуючи оплату, передає криптоактиви на гаманець зловмисника. Хоча потерпілий у цьому разі втрачає грошові кошти, проте умисел винного спрямований саме на заволодіння криптоактивами за рахунок оплати їхньої покупки потерпілим.

Заволодіння криптоактивами шляхом обману чи зловживання довірою за своєю природою є типовими видами шахрайства, які часто є майже ідентичними до тих, що застосовуються при заволодінні грошовими коштами або іншим рухомим майном.

Розвиток криптоекосистеми також зумовив адаптацію та модифікацію наявних схем інвестиційного шахрайства, серед яких найпопулярнішими є шахрайство з виходом (англ. Exit Scam), фінансові піраміди (англ. Ponzi schemes) та гібридне інвестиційне шахрайство [16].

2.1. Шахрайство з виходом

У 2017–2018 рр. на крипторинку набув широкого застосування такий механізм для залучення інвестицій, як ICO (з англ. initial coin offering – первинна пропозиція монети) та похідних від нього: IDO (з англ. initial DEX offering – первинна децентралізовано-біржова пропозиція), IEO (з англ. initial exchange offering – первинна біржова пропозиція). Не вдаючись у специфічні деталі кожного з цих видів інвестування, зазначимо, що ICO передбачає залучення розробниками певного криптопроєкту інвестиційного капіталу у вигляді грошових коштів чи ліквідних криптоактивів (наприклад, Bitcoin або USDT), в обмін на що інвестори отримують новостворені розробниками токени (які, за очікуванням інвесторів, у майбутньому мають зрости в ціні).

Через новизну ринку та слабке правове регулювання ICO часто використовувалось як механізм для шахрайства: зловмисники робили «видимість» розроблення певного крипто-проєкту, запускаючи маркетингові акції, створюючи вебсайти та документацію, які описували довготривалі плани розвитку проєкту. Такі дії вчинялись із метою введення потерпілих (інвесторів) в оману шляхом створення у них враження щодо перспективності та прибутковості їхніх інвестицій. Одразу після збору інвесторського капіталу розробники обертали його на свою користь (робили «вихід»), не здійснюючи реальних дій із розробки токену, і просто зникали.

Одним із найбільш відомих випадків шахрайства на ICO є справа «OneCoin». Згідно з обвинувальним актом на інвестиціях в неіснуючий токен «OneCoin» група осіб змогла заволодіти більш як 4 мільярдами доларів США [17, с. 5].

2.2. Фінансові піраміди

Схеми фінансових пірамід існують вже понад сто років, і криптосфера не стала винятком для їхнього поширення. Організатори таких схем створюють ілюзію ведення прибуткового високотехнологічного бізнесу (хмарний майнінг криптоактивів, розробка торгових ботів на основі штучного інтелекту, стейкінг з високовідсотковим доходом тощо), який потребує залучення інвестицій (криптоактивів) із подальшим поверненням цих інвестицій із відсотками. Насправді ж, виплата відсотків (прибутку) попереднім інвесторам здійснюється виключно за рахунок залучення криптоактивів нових вкладників. Повернення інвестицій та прибутку первинним вкладникам допомагає організаторам здійснювати обман нових вкладників, створюючи у них помилкову переконаність в успішності та працездатності моделі бізнесу та, як наслідок, вигідності їхньої інвестиції. На етапі, коли суми виплат починають перевищувати суму надходжень нових інвестицій, організатори піраміди, як правило, припиняють виплати та зникають із залишком залучених інвестицій.

Яскравим прикладом реалізації такої пірамідальної схеми є справа платформи BitConnect. Механізм шахрайства базувався на дворівневій системі залучення активів: інвесторам пропонувалося придбати нативний токен платформи (BCC) за Bitcoin, після чого передати ці токени в «програму кредитування» під обіцянку гарантованого пасивного доходу до 1 % на день, який нібито генерувався спеціальним торговим ботом. Фактично ж залучені Bitcoin акумулювалися організаторами, а виплати «прибутку» здійснювалися за рахунок нових надходжень. Як у подальшому встановило Федеральне бюро розслідувань США, загальний обсяг криптоактивів, якими заволоділи організатор схеми та його співучасники, перевищив 2 мільярди доларів США [18].

2.3. Гібридне інвестиційне шахрайство

Гібридне інвестиційне шахрайство – це доволі «молодий» вид шахрайства, об'єктивна сторона якого на різних етапах свого виконання передбачає комбінування двох способів заволодіння майном: обману та зловживання довірою.

На початковому етапі реалізації кримінального протиправного умислу зловмисник створює фіктивну цифрову особистість. Використовуючи сервіси

знайомств, соціальні мережі, месенджери, зловмисник встановлює контакт із потерпілим, видаючи себе за сексуально привабливу для потерпілого особу або ж потенційного друга. На цій стадії обман в особі має підготовчий характер і спрямований не на безпосереднє заволодіння майном, а на формування в свідомості потерпілого відчуття довіри до цифрової особистості зловмисника.

На наступному етапі зловмисник, зловживаючи довірою потерпілого, переконує останнього у вигідності певного виду заробітку. Зловживання довірою може поєднуватись на цьому етапі з обманом: потерпілому може надаватися доступ до вебресурсів (фейкових сайтів чи програм), які були заздалегідь створені та налаштовані зловмисником для імітації успішного інвестування.

На заключному етапі для формування у потерпілого остаточного хибного переконання у реальності заробітку, зловмисник часто спонукає потерпілого здійснити купівлю незначної кількості криптоактивів та зробити пробну інвестицію незначного обсягу (при цьому, придбання криптоактивів потерпілим часто може здійснюватись на цілком законних платформах з подальшим переказом криптоактивів на гаманці, які належать зловмиснику). Після отримання фіктивного прибутку потерпілому дозволяють безперешкодно вивести його. Коли під впливом сформованої ілюзії успіху потерпілий інвестує максимально можливу суму, реалізується фінальна фаза кримінального правопорушення: доступ до виведення активів раптово блокується зловмисником [19, с. 5]. Іноді також можливе продовження кримінального правопорушення, коли зловмисник намагається заволодіти додатковими активами жертви під вигаданими приводами: необхідність сплати податків, комісії за вивід прибутку тощо.

У публіцистичній та науковій літературі такий вид шахрайства отримав декілька назв: крипторoман (анг. cryptorom), романтичне заманювання (англ. romance baiting), проте найбільш поширеною назвою є «забій свиней» (англ. pig butchering). Цей термін має китайське походження (Shā Zhū Pán), і його етимологія базується на метафорі з «відгодовуванням свині» (тривалий процес формування довіри, створення переконаності у вигідності інвестицій) та «забоєм» (фінальне заволодіння «інвестованими» потерпілим криптоактивами) [19, с. 3]. При цьому термін Pig butchering вже став сталим виразом в англомовному середовищі й уживається навіть державними органами (наприклад, Каліфорнійським департаментом фінансового захисту та інновацій) [20].

Наведені приклади ілюструють лише окремі прояви обманних викрадень криптоактивів. Насправді ж варіативність злочинних сценаріїв є значно

ширшою. Такі «схеми» можуть бути як примітивними (фіктивні збори криптоактивів на благодійність, продаж неіснуючих товарів або послуг тощо), так і складними, які одночасно поєднують обман в особі, обман в намірах та інші види обману.

3. Привласнення, розтрата або заволодіння криптоактивами шляхом зловживання службовим становищем

Ще однією групою традиційних посягань на відносини власності на криптоактиви є привласнення, розтрата та заволодіння криптоактивами шляхом зловживання службовим становищем. Поширеність таких способів посягань у криптосфері зумовлена специфічними умовами її сьогоденного існування.

Початкова ідеологія криптоактивів була заснована на принципі децентралізації. Цей принцип передбачав: відсутність центрального емітента валюти; відсутність центрального органу, що здійснює контроль за транзакціями; можливість здійснювати криптоплатежі без участі посередників [21, с. 129].

Хоча ідеологія блокчейну і ґрунтується на принципі децентралізації, в сучасних умовах значна частина криптотранзакцій здійснюється через централізованих посередників (криптобіржі, професійні трейдери, інвестиційні фонди, кастодіальні сервіси тощо). Через таку специфіку крипторинку велика кількість криптоактивів, що є в обігу, перебуває у володінні, користуванні чи на зберіганні у третіх осіб.

Наприклад, зберігаючи криптоактиви на кастодіальному гаманці, власник фактично уповноважує адміністраторів такого кастодіального сервісу здійснювати зберігання його криптоактивів та виконувати транзакції з ними за його дорученням. В іншому прикладі, передаючи криптоактиви в управління трейдеру чи інвестиційному фонду, власник доручає останнім здійснювати право розпорядження своєю власністю.

Саме чинник концентрації фактичного контролю над криптоактивами в руках третіх осіб створює підґрунтя для вчинення кримінальних правопорушень у вигляді привласнення, розтрати чи заволодіння криптоактивами шляхом зловживання службовим становищем.

Механізм посягання в цьому разі полягає в тому, що суб'єкт кримінального правопорушення (директор біржі, криптотрейдер, управитель інвестиційного фонду), маючи законний доступ до приватних ключів або системи управління транзакціями, або безпосередньо здійснюючи права володіння чи розпорядження криптоактивами, вчиняє дії щодо їх привласнення чи розтрати.

Не вдаючись у специфіку розмежування складів кримінальних правопорушень у вигляді привласнення, розтрати чи заволодіння майном шляхом

зловживання службовим становищем, зазначимо, що суб'єкт у таких кримінальних правопорушеннях завжди здійснює спеціальні повноваження щодо криптоактивів (вони безпосередньо йому ввірені в рамках тих чи інших правовідносин, перебувають у його віданні або ж ввірені чи перебувають у віданні підконтрольних йому осіб) [3, с. 247, 255].

Справа криптобіржі FTX є найбільш відомим прикладом, що якнайкраще ілюструє механізм привласнення та розтрати ввірених криптоактивів: Окружний суд Південного округу Нью-Йорка призначив колишньому власнику та генеральному директору криптобіржі FTX покарання у вигляді 25 років позбавлення волі. В основу обвинувачення було покладено, зокрема те, що частина клієнтських активів (яка еквівалентна декільком мільярдам доларів) витрачалась на особисті потреби генерального директора, його інвестиції та покриття боргів [22; 23, с. 290–291].

Потрібно наголосити, що привласнення, розтрату чи заволодіння криптоактивами шляхом зловживання службовим становищем (частини 1, 2 ст. 191 КК) слід відрізняти від суміжних складів кримінальних правопорушень, зокрема шахрайства (ст. 190 КК). Так, передача криптоактивів в управління трейдеру, який здійснює обернення таких криптоактивів на свою користь одразу в момент їх отримання від власника, слід кваліфікувати як шахрайство, оскільки суб'єкт кримінального правопорушення в такому випадку від самого початку не має наміру виконувати взяті на себе зобов'язання щодо управління активами. Його дії спрямовані на те, щоб під виглядом надання послуг трейдингу (торгівлі криптоактивами з метою отримання прибутку) заволодіти майном потерпілого. У такій ситуації укладення договору про управління чи обіцянка здійснювати трейдинг є лише способом обману. Для кваліфікації ст. 191 КК (як привласнення чи розтрати майна) необхідною умовою є те, що майно було ввірене винному на законних підставах, і умисел на його привласнення чи розтрату виник вже після встановлення правовідносин під час здійснення повноважень з управління цим майном.

Розтрату ввірених криптоактивів також слід відрізняти від інших діянь, які хоча формально й схожі на кримінальне правопорушення, проте ним не є. Йдеться насамперед про випадки втрати активів унаслідок нормального господарського ризику або невдалої торгової діяльності. Якщо управитель (трейдер, розпорядник фонду), діючи в межах наданих йому повноважень, втратив ввірені криптоактиви через різку зміну ринкового курсу (волатильність), кримінальна відповідальність виключається. Такі дії або бездіяльність можуть розглядатись виключно у площині цивільно-правових відносин як, можливо, неналежне виконання договірних зобов'язань.

II. Нетрадиційні способи посягання

До другої групи способів протиправного посягання на відносини власності на криптоактиви пропонується віднести діяння, вчинення яких стає можливим виключно завдяки використанню специфічних технічних засобів, шкідливого програмного забезпечення або експлуатації вразливостей архітектури блокчейн-мереж. Такі способи посягань відрізняються від традиційних за низкою ознак:

– за об'єктом: крім основного об'єкта (відносин криптовласності), додатковим об'єктом посягання є нормальне функціонування електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж;
– за об'єктивною стороною: у зазначених кримінально протиправних посяганнях вона завжди має «технічну складову» – заволодіння криптоактивами відбувається внаслідок втручання в роботу комп'ютерів, використання шкідливого програмного забезпечення чи експлуатації вразливостей програмних протоколів[1].

Нижче будуть розглянуті найбільш поширені нетрадиційні способи посягань проти криптовласності.

1. Викрадення криптоактивів за допомогою шпигунського програмного забезпечення

Поява криптовласності неминуче вплинула на трансформацію механізму кримінально протиправного заволодіння нею. Якщо у випадку класичної крадіжки метою зловмисника є фізичне вилучення речі матеріального світу з володіння власника, то у сфері криптоактивів фізичне вилучення неможливе. Криптоактив не існує у фізичному просторі (у його класичному кримінально-правовому розумінні), його не можна «забрати» чи перемістити до своєї кишені, а тому протиправна діяльність зловмисників спрямовується на заволодіння засобами доступу до цих активів.

Архітектура блокчейнмереж побудована так, що система не ідентифікує особу користувача, а перевіряє лише валідність цифрового підпису, який генерується за допомогою приватного ключа. Це створює ситуацію, за якої фактичне володіння унікальним набором даних (приватним ключем, seed-фразою) і є підтвердженням володіння криптоактивами. Такий підхід використаний і українським законодавцем у ст. 6 Закону України «Про віртуальні активи» [24].

[1] Особа правопорушника характеризується тим, що він, як правило, володіє спеціальними знаннями та навичками у сфері комп'ютерних технологій.

Тож вилучення активів поза волею власника стає можливим лише за умови попереднього заволодіння відповідним засобом доступу (приватним ключем, seed-фразою, паролем). Саме отримання цих даних є обов'язковою передумовою для подальшого незаконного обернення активів на користь зловмисника.

Цінність засобів доступу (приватний ключ, seed-фраза, пароль) детермінувала зміну знарядь вчинення кримінального правопорушення. Оскільки ці засоби зазвичай зберігаються у цифровій формі на пристроях користувачів, фізичні методи вчинення крадіжок втратили свою актуальність для відповідного предмета посягання. Натомість виникла необхідність в інструментах, здатних дистанційно та непомітно для власника проникати в операційну систему, знаходити потрібні файли та копіювати їх. Наведене стало каталізатором розробки та стрімкого поширення спеціалізованого шпигунського програмного забезпечення (англ. spyware), найбільш поширеними видами якого є кейлогери (англ. keyloggers) та стілери (англ. stealers).

Кейлогер – це клас шкідливого програмного забезпечення, призначеного для прихованої фіксації та збереження натискань клавіш комп'ютера з подальшою їх передачею зловмиснику [25, с. 1]. Основною метою кейлогерів є перехоплення seed-фрази або паролів у момент їх ручного введення користувачем комп'ютера. У свою чергу, стілер – це клас шкідливого програмного забезпечення, основною метою якого є пошук у пам'яті комп'ютера або перехоплення під час відправки файлів чи даних, у яких збережені ключі, seed-фраза та пароль, та подальша дистанційна передача таких файлів зловмиснику. Так, наприклад, компанія Microsoft у 2025 р. повідомила про новий вид шкідливого програмного забезпечення – StilachiRAT, який сканує комп'ютер на предмет наявності розширень криптогаманців для Google Chrome та здійснює пошук облікових даних, зокрема паролів для доступу до цих гаманців [26].

Складна технічна природа викрадень криптоактивів за допомогою шпигунського програмного забезпечення викликає труднощі у правильній кримінально-правовій кваліфікації таких діянь та розмежуванні їх між собою (у тому числі крадіжки та шахрайства). Зокрема викликає інтерес кримінально-правова оцінка використання зловмисником викрадених засобів доступу (приватних ключів, паролів) до криптоактивів.

У кримінально-правовій доктрині обман як ознака шахрайства полягає у повідомленні потерпілому (власнику або особі, якій ввірене чи під охороною якої перебуває майно, або особі, яка має доступ до нього) неправдивої інформації або приховування тієї інформації, яка мала би бути йому пові-

домлена, з метою введення потерпілого в оману, схилення його до певної поведінки (зумовленою такою оманою) та заволодіння його майном чи набуття права на нього [2, с. 401].

Потреба у застосуванні обману як засобу заволодіння криптоактивами безпосередньо корелює з технічними особливостями програмної архітектури, за допомогою якої здійснюється розпорядження криптоактивами. Ключовим питанням тут є те, чи вимагає платіжна програмна інфраструктура підтвердження особистості (ідентифікації) ініціатора транзакції, чи обмежується лише перевіркою валідності криптографічних ключів.

Переважна більшість кастодіальних криптосервісів (централізовані біржі, криптобанки тощо) передбачає обов'язкову ідентифікацію користувача (власника криптоактивів) для надання йому послуг, зокрема зі зберігання його криптоактивів та проведення транзакцій із ними. Наприклад, найбільша в світі на час написання цієї статті криптобіржа Binance вимагає обов'язкового проходження процедури ідентифікації користувача, що включає надання особистих документів, підтвердження адреси, номеру телефона, електронної пошти тощо [27].

Отже, у разі якщо суб'єкт кримінального правопорушення використовує викрадені паролі для доступу до облікових записів на кастодіальних (централізованих) сервісах, він фактично вводить в оману адміністратора такого сервісу. Використовуючи обман в особі та видаючи себе за законного власника криптоактивів (користувача платформи), зловмисник спонукає кастодіальний сервіс виконати розпорядження на здійснення транзакції. У цьому разі об'єктом обману є адміністратор відповідного сервісу, який помилково, сприймаючи зловмисника за законного власника криптоактивів, приймає рішення про здійснення транзакції. Хоча таке рішення і приймається в автоматизований спосіб за допомогою налаштованих технічних алгоритмів, виконання цього алгоритму санкціоноване безпосередньо адміністратором кастодіального сервісу, а необхідною умовою його виконання стає успішна імітація зловмисником особи законного власника.

Тож викрадення засобів доступу до облікового запису на кастодіальному сервісі за допомогою шпигунського програмного забезпечення та подальше обернення активів на свою користь (шляхом авторизації під виглядом власника та ініціювання транзакції) слід кваліфікувати як шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 4 ст. 190 КК), та несанкціоноване втручання в роботу інформаційних (автоматизованих) систем (ст. 361 КК). Розробка шкідливого програмного забезпечення та його розповсюдження серед потенційних потерпілих також потребує кваліфікації за ст. 361[1] КК.

Кардинально іншою є правова природа діяння при заволодінні активами, що зберігаються на некастодіальних гаманцях, які функціонують у децентралізованих мережах.

В архітектурі більшості блокчейнів відсутній єдиний адміністратор або керуючий орган, уповноважений перевіряти транзакції. Підтвердження операцій здійснюється децентралізованою мережею валідаторів винятково на основі математичних алгоритмів консенсусу. При цьому протокол блокчейну не передбачає ідентифікації особи ініціатора транзакції. Для системи наявність валідного цифрового підпису, згенерованого приватним ключем, є абсолютною та достатньою підставою для переказу криптоактивів. Підтверджуючи транзакцію, валідатори не сприймають інформацію про особу власника, а лише перевіряють криптографічну коректність ключа.

Відповідно, використовуючи приватний ключ від криптогаманця іншої особи в некастодіальних системах, зловмисник не застосовує обман, оскільки відсутня особа, яку обманюють: валідатори транзакції не перевіряють особу власника криптоактивів, і в силу програмного рішення не повинні і не можуть цього робити, а особою, яка ініціює транзакцію, може бути будь-хто.

Тому, на наш погляд, викрадення криптоактивів з некастодіальних гаманців за допомогою попередньо викрадених ключів слід кваліфікувати як крадіжку (ст. 185 КК) та несанкціоноване втручання в роботу інформаційних (автоматизованих) систем (ст. 361 КК).

Іншою проблемою кримінально-правової кваліфікації «шпигунських викрадень» криптоактивів є визначення моменту закінчення кримінального правопорушення. Зокрема, потребує з'ясування питання, якій стадії вчинення кримінального правопорушення відповідає момент фактичного отримання зловмисником засобів доступу до криптоактивів (приватного ключа, seed-фрази, пароля). Специфіка використання шкідливого програмного забезпечення часто створює часовий розрив між перехопленням інформації та фактичним вилученням активів. У зв'язку з цим виникає потреба у з'ясуванні того, чим, згідно з кримінальним законом, є факт заволодіння засобами доступу (приватним ключем, seed-фразою)?

По суті, такі об'єкти виступають *цифровими легітимаційними знаками*. Як правильно зазначає Н. О. Антонюк, легітимаційні знаки посвідчують право на одержання майна [28, с. 280], а коли йдеться про їх традиційні різновиди, то вони можуть виступати як предметом кримінального правопорушення проти власності (наприклад, картки на поповнення мобільного рахунку), так і засобом його вчинення (квитанція, накладна і т. ін.) [28, с. 283]. Цифрові ж легітимаційні знаки належать саме до тієї групи знаків, які слугують

засобом вчинення кримінального правопорушення, адже сам по собі набір символів (ключ) не є майновим благом, і заволодіння цим ключем не є самоціллю зловмисника. Викрадення засобу доступу за допомогою шпигунського програмного забезпечення є етапом реалізації кримінально протиправного умислу винного, спрямованого на обернення криптоактивів на свою користь.

Оскільки заволодіння ключем є лише проміжною дією перед майбутнім заволодінням криптоактивами, такі дії (до моменту фактичного ініціювання транзакції) слід кваліфікувати як незакінчений замах на крадіжку (ст. 185 КК) або шахрайство (ст. 190 КК) та закінчене несанкціоноване втручання в роботу інформаційних (автоматизованих) систем (ст. 361 КК).

2. Викрадення криптоактивів через підміну платіжних реквізитів

До окремої підгрупи нетрадиційних способів викрадення криптоактивів можна віднести викрадення через підміну платіжних реквізитів (адресу криптогаманців). Об'єктивна сторона цих посягань характеризується тим, що суб'єкт кримінального правопорушення реалізує свій умисел не шляхом заволодіння засобами доступу до криптоактивів, а шляхом підміни адреси криптогаманця отримувача. Здійснюючи підміну адреси криптогаманця, зловмисник використовує складність блокчейн-адрес, які через свій значний обсяг та складну структуру є складними для запам'ятовування чи візуальної перевірки потерпілим. Найбільш поширеними засобами підміни платіжних реквізитів є такі:

1) кліпери (англ. Clippers). За даними криптобіржі Binance, цей різновид шкідливого програмного забезпечення функціонує шляхом несанкціонованої модифікації вмісту буфера обміну операційної системи комп'ютера. Механізм дії полягає у такому: коли користувач (власник криптоактивів) копіює адресу гаманця для здійснення переказу, кліпер миттєво замінює оригінальні реквізити на адресу, підконтрольну зловмиснику [29]. Якщо при підтвердженні транзакції користувач не звірить скопійований набір символів із тим, що був вставлений у поле «Отримувач», криптоактиви будуть безповоротно надіслані на гаманець зловмисника;
2) отруєння адреси (англ. Address Poisoning). Підміна платіжних реквізитів шляхом «отруєння адреси» не передбачає використання шкідливого програмного забезпечення, а використовує фактор неуважності з боку потерпілого. Механізм реалізації об'єктивної сторони полягає в тому, що зловмисник, використовуючи спеціалізоване програмне забезпечення, здійснює моніторинг блокчейну для пошуку криптогаманця, з якого перекази часто здійснюються на ту саму адресу.

> Виявивши адресу, на яку потерпілий часто здійснює перекази, злочинець створює власну «адресу-двійника», яка візуально нагадує оригінальну адресу (як правило, перші та останні декілька символів повністю збігаються з адресою реального контрагента потерпілого). Після створення адреси-двійника зловмисник надсилає на гаманець потерпілого транзакцію з мізерною сумою, внаслідок чого в історії транзакцій потерпілого з'являється запис адреси-двійника, яка виглядає подібно до адреси постійного контрагента. Розрахунок робиться на те, що при наступному переказі потерпілий, замість ручного введення, скопіює адресу отримувача безпосередньо з історії транзакцій (оскільки вона є останньою у списку), помилково сприйнявши адресу зловмисника за адресу перевіреного контрагента [30, с. 1243].

В обох наведених вище випадках переказ криптоактивів злочинцю є результатом добровільного волевиявлення потерпілого, який самостійно здійснює транзакцію. Однак волевиявлення власника є дефектним і не відповідає його справжній волі, оскільки в момент здійснення транзакції потерпілий перебуває під впливом обману, помилково вважаючи, що здійснює переказ криптоактивів на відомий йому криптогаманець, тоді як фактично відправляє їх зловмиснику. Отже, заволодіння криптоактивами через підміну платіжних реквізитів слід кваліфікувати як шахрайство, вчинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки (ч. 4 ст. 190 КК).

Під час кваліфікації також потрібно враховувати використаний суб'єктом кримінального правопорушення інструментарій. У разі використання кліперів таке шахрайство утворює ідеальну сукупність з несанкціонованим втручанням у роботу інформаційних систем і потребує додаткової кваліфікації за ст. 361 КК, оскільки об'єктивна сторона кримінального правопорушення виконується шляхом несанкціонованого встановлення шкідливого програмного забезпечення на комп'ютер потерпілого та підміни даних його буфера обміну.

Дії винного, пов'язані з підготовкою до вчинення кримінального правопорушення (створення шкідливого програмного забезпечення, його розповсюдження), також повинні додатково кваліфікуватись за ст. 361[1] КК як створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут.

Якщо ж заволодіння криптоактивами було здійснено за допомогою отруєння адреси, то дії винного не потребують додаткової кваліфікації за ст. 361 КК, оскільки втручання в роботу комп'ютера потерпілого не відбувається.

3. Шахрайство з використанням «підроблених» криптоактивів

Програмні особливості функціонування блокчейнів дозволяють будь-якій особі створити власний токен. При цьому назва такого токена та його символ необов'язково мають бути унікальними та можуть повністю чи частково повторювати назви відомих криптоактивів [31, с. 50:5].

Такі технічні особливості існування криптоактивів стали умовою для створення зловмисниками токенів-клонів, які в подальшому використовуються для розрахунку з потерпілим (як правило, при обміні криптоактивів на децентралізованих платформах). Потерпілий, бажаючи здійснити обмін, отримує «клоновані» криптоактиви. Оскільки більшість інтерфейсів некастодіальних криптогаманців ідентифікують токен насамперед за його символом та логотипом, потерпілий помилково сприймає ці токени-клони як справжній ліквідний актив. Під впливом такої візуальної ілюзії потерпілий вважає, що отримав оплату і передає свої криптоактиви (наприклад, Bitcoin) зловмиснику, фактично обмінюючи ліквідний актив на токени-клони, які не мають жодної ринкової вартості.

Заволодіння майном потерпілого шляхом використання токенів-клонів слід кваліфікувати як шахрайство. У цьому випадку має місце обман у предметі: потерпілому передається криптоактив, який не відповідає тим властивостям (зокрема ліквідності та міновій вартості) справжнього криптоактиву, про передачу якого домовлялися сторони.

При цьому вищеописані дії винного містять ознаки кваліфікованого складу шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 4 ст. 190 КК), оскільки реалізація об'єктивної сторони та обман потерпілого здійснюються з використанням програмного коду для створення токену-клону.

Водночас такі дії винного не потребують кваліфікації за статтями розд. XVI КК, оскільки створюючи токен-клон, винний використовує передбачений розробниками функціонал блокчейн-мережі і не здійснює несанкціонованого втручання в роботу системи чи пристрою потерпілого.

Важливо наголосити, що дії винного зі створення токену-клону також не утворюють складів кримінальних правопорушень, передбачених ст. 199 КК (виготовлення підроблених грошей) або ст. 200 КК (підробка електронних грошей), оскільки криптоактиви не мають правового режиму валюти, грошових коштів або електронних грошей, а тому не можуть виступати предметом зазначених кримінальних правопорушень.

4. Викрадення криптоактивів із використанням вразливостей програмного коду

Окремою групою способів заволодіння криптоактивами, що характеризується найвищим рівнем технічної складності, є використання вразливостей у програмному коді смарт-контрактів. Смарт-контракт за своєю сутністю є сукупністю умов договору, що записані у програмний код, які автоматично виконують операції з криптоактивами за наперед визначеним алгоритмом [32, с. 40].

Вплив людського фактора на етапі розробки смарт-контрактів зумовлює ризик виникнення програмних вразливостей, використання яких дозволяє зловмисникам маніпулювати роботою протоколу та протиправно заволодівати криптоактивами. Враховуючи стрімку еволюцію технологій, сформувати вичерпний перелік технічних способів злому не видається можливим. Архітектура смарт-контрактів постійно ускладнюється, що неминуче призводить до виникнення нових, специфічних способів використання вразливостей програмного коду.

Проте історія становлення крипторинку знає декілька хрестоматійних прикладів, які дозволяють зрозуміти механіку та масштаб суспільної небезпеки таких діянь. Одним із найбільш показових випадків є злом децентралізованого венчурного фонду The DAO (англ. «The DAO Hack»). Так, у 2016 р. хакер (або група хакерів) використали помилку в логіці виконання смарт-контракту, сутність якої полягала в тому, що алгоритм контракту порушував належну послідовність дій: вивід криптоактивів здійснювався до оновлення балансу користувача. Зловмисник скористався цією особливістю, ініціювавши багаторазові повторні виклики функції виведення активів у межах однієї транзакції. Оскільки баланс у системі залишався незмінним до завершення всіх викликів, смарт-контракт щоразу помилково визнавав наявність активів на балансі для їхнього виведення. Унаслідок цього зловмиснику вдалося багаторазово отримати активи, які формально ще не були списані з його рахунку, що призвело до незаконного виведення криптоактивів Ethereum на суму, що на той час була еквівалентна 60 мільйонам доларів США [33, с. 25:6].

Специфіка подібного роду зломів полягає в тому, що зловмисник взаємодіє виключно з програмним середовищем і не здійснює безпосередній вплив на потерпілого. Тож такі дії не можуть кваліфікуватися як шахрайство, оскільки обов'язковою ознакою шахрайства є обман, адресований людині, який у цьому разі не здійснюється.

Отже, зазначені діяння, як правило, мають кваліфікуватися як крадіжка (ст. 185 КК), утворюючи ідеальну сукупність із несанкціонованим втручанням у роботу інформаційних (автоматизованих) систем (ст. 361 КК).

Висновки

Стрімке зростання цінності криптоактивів має своїм закономірним наслідком збільшення кількості кримінально протиправних посягань, предметом яких вони є. Способи таких посягань набули широкого різноманіття: від найпримітивніших форм насильницьких викрадень до технічно складних та добре продуманих злочинних схем, реалізація яких передбачає застосування шкідливого програмного забезпечення чи експлуатацію вразливостей архітектури блокчейн-мереж.

Умовно способи вчинення кримінальних правопорушень проти криптовласності можна поділити на дві групи: традиційні та нетрадиційні.

Перша група охоплює способи, які є універсальними для більшості корисливих посягань на власність. Реалізація об'єктивної сторони таких діянь не детермінована технологічною специфікою предмета посягання: криптоактиви розглядаються злочинцем тотожно до грошових коштів чи іншого майна. При цьому злочинні схеми є стандартними і лише частково можуть модифікуватись, враховуючи цифрове середовище існування криптоактивів.

До цієї групи належать насильницькі викрадення (які, залежно від обставин, можуть кваліфікуватись як насильницький грабіж, розбій або вимагання), різноманітні форми шахрайства (фінансові піраміди, інвестиційні схеми), а також привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем.

Другу групу становлять нетрадиційні способи, реалізація яких стає можливою виключно завдяки використанню специфічного технічного інструментарію чи особливостей архітектури блокчейну. Специфікою цієї групи є застосування високотехнологічного злочинного інструментарію – від перехоплення конфіденційних даних потерпілого (seed-фрази, пароля тощо) та підміни адрес отримувачів до технічно складних втручань у роботу децентралізованих протоколів.

Визначальним критерієм для розмежування складів кримінальних правопорушень, які вчиняються нетрадиційним способом, є наявність дефекту волі у потерпілого чи іншої особи (яка уповноважена потерпілим на зберігання його криптоактивів). Якщо заволодіння активами відбувається внаслідок обману або зловживання довірою, коли потерпілий унаслідок інформаційного впливу на його психіку сам здійснює розпорядження майном (вважаючи це вигідним або необхідним), дії винного слід кваліфікувати як шахрайство, вчинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки (ч. 4 ст. 190 КК). Натомість, якщо заволо-

діння відбувається поза волею власника (шляхом викрадення seed-фрази, використання шкідливого програмного забезпечення, втручань у роботу програмного коду), такі діяння, як правило, утворюють склад крадіжки. У випадках, коли викрадення вчиняється у поєднанні із застосуванням технічних засобів втручання в роботу інформаційних (автоматизованих) систем, такі дії також потребують додаткової кваліфікації за ст. 361 КК.

Правильне розуміння природи способу вчинення кримінального правопорушення проти криптовласності є ключем до його правильної кваліфікації, що дозволяє уникнути помилок під час правового оцінювання діянь та сприятиме формуванню єдиної правозастосовної практики. Запропоновані підходи до класифікації відповідних способів і кваліфікації посягань на криптовласність можуть забезпечити ефективне застосування чинних норм кримінального закону до новітніх викликів кіберзлочинності, стаючи запорукою дієвого захисту власності в умовах стрімкого зростання популярності криптоактивів.

Список використаних джерел

[1] Coingecko: 2025 Q3 Crypto Industry Report. URL: https://www.coingecko.com/research/publications/2025-q3-crypto-report (last accessed: 17.05.2026).
[2] Кримінальне право (Особлива частина) : підручник / за ред. О. О. Дудорова, Є. О. Письменського. Луганськ : Елтон-2, 2012. Т.1. 780 с.
[3] Антонюк Н. О. Кримінально-правова охорона власності : навч. посіб. / ЛНУ ім. Івана Франка. Львів, 2012. 514 с.
[4] Демидова Л. Безтілесна річ як предмет злочину. *Вісник Національної академії правових наук України*. 2015. № 2(81). С. 101–108.
[5] Дорохіна Ю. А. Злочини проти власності. Теоретико-правове дослідження : монографія. Київ : Київ. нац. торг.-екон. ун-т, 2016. 744 с.
[6] Кришевич О. В., Рощина І. О. Криптовалюта, як предмет кримінального правопорушення проти власності: національне та міжнародне законодавство. *Вісник Маріупольського державного університету. Серія: Право*. 2022. Вип. 23–24. С. 168–175. https://doi.org/10.34079/2226-3047-2022-12-23-24-168-175.
[7] Думчиков М. О. Особливості кваліфікації шахрайства в кіберпросторі, засобом вчинення якого є віртуальні активи. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія: Право*. 2022. № 14(26). С. 159–165. https://doi.org/10.33098/2078-6670.2022.14.26.149-155.
[8] Kozii V. Criminal liability for illegal possession of cryptocurrency in Ukraine. *Social & Legal Studios*. 2023. Vol. 6, No. 1. P. 33–40. https://doi.org/10.32518/sals1.2023.33.
[9] Щеглаков І. Е. Проблеми розмежування криптотермінів при кваліфікації кримінальних правопорушень проти власності. *Вісник Асоціації кримінального права України*. 2025. № 1(23). С. 225–246. https://doi.org/10.21564/2311-9640.2025.23.331560.
[10] Ordekian M., Atondo-Siu G., Hutchings A., Vasek M. Investigating Wrench Attacks: Physical Attacks Targeting Cryptocurrency Users. *6th Conference on Advances in Financial Technologies (AFT 2024)*. 2024. P. 24:1–24:24. https://doi.org/10.4230/LIPIcs.AFT.2024.24.

[11] TRM Labs: The Rise of Wrench Attacks and Crypto-related Violent Crime. URL: https://www.trmlabs.com/resources/blog/the-rise-of-wrench-attacks-and-crypto-related-violent-crime (last accessed: 17.05.2026).
[12] Вирок Обухівського районного суду Київської області від 06.12.2022 р. у справі № 761/31532/21. URL: https://reyestr.court.gov.ua/Review/107735753 (дата звернення: 17.05.2026).
[13] Київська міська прокуратура: У Києві затримали чотирьох псевдоправоохоронців, які погрозами змусили криптобізнесмена перерехувати їм 250 тисяч доларів США. URL: https://kyiv.gp.gov.ua/ua/news.html?_m=publications&_c=view&_t=rec&id=368660 (дата звернення: 17.05.2026).
[14] Вирок Оболонського районного суду міста Києва від 10.12.2024 р. у справі №756/12186/24. URL: https://reyestr.court.gov.ua/Review/123696369 (дата звернення: 17.05.2026).
[15] Вирок Саратського районного суду Одеської області від 23.10.2024 р. у справі № 513/1179/24. URL: https://reyestr.court.gov.ua/Review/122489352 (дата звернення: 17.05.2026).
[16] Tiwari M., Lupton C., Bernot A., Halteh Kh. The cryptocurrency conundrum: the emerging role of digital currencies in geopolitical conflicts. *Journal of Financial Crime*. 2024. No. 31(6). P. 1622–1634. https://doi.org/10.1108/JFC-12-2023-0306.
[17] Watters C. When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment. *MDPI: Laws*. 2023. No. 12 (2). P. 1–16. https://doi.org/10.3390/laws12020033.
[18] U.S. Department of Justice: BitConnect Founder Indicted in Global $2.4 Billion Cryptocurrency Scheme. URL: https://www.justice.gov/archives/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme (last accessed: 17.05.2026).
[19] Maras M.-H., Ives E.R. Deconstructing a form of hybrid investment fraud: Examining 'pig butchering' in the United States. *Journal of Economic Criminology*. 2024. No. 5(3):100066. P. 1–19. https://doi.org/10.1016/j.jeconc.2024.100066.
[20] The Department of Financial Protection and Innovation: Pig butchering – how to spot and report the scam. URL: https://dfpi.ca.gov/news/insights/pig-butchering-how-to-spot-and-report-the-scam/ (last accessed: 17.05.2026).
[21] Іщеглаков І. Філософсько-правові проблеми децентралізації криптовалют. *Філософія і право* : тези доп. Міжнар. наук. конф. асп. та студ. (м. Харків, 21 трав. 2025 р.) Харків, 2025. С. 128–130.
[22] United States Attorney's Office. Southern District of New York: Samuel Bankman-Fried Sentenced to 25 Years in Prison. URL: https://www.justice.gov/usao-sdny/pr/samuel-bankman-fried-sentenced-25-years-prison (дата звернення: 17.05.2026).
[23] Mackenzie S. Crypto collapse: the cult of personality and the normalisation of fraud in FTX and Celsius. *Journal of Financial Crime*. 2025. Vol. 32, issue 6. P. 288–303. https://doi.org/10.1108/JFC-01-2024-0054.
[24] Про віртуальні активи : Закон України від 17.02.2022 р. № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20 (дата звернення: 28.02.2026).
[25] Singh A., Choudhary P., Singh A. K., Tyagi D. K. Keylogger Detection and Prevention. *Journal of Physics: Conference Series*. 2021. Vol. 2007(1). P. 1–8. https://doi.org/10.1088/1742-6596/2007/1/012005.
[26] Microsoft: StilachiRAT analysis: From system reconnaissance to cryptocurrency theft. URL: https://www.microsoft.com/en-us/security/blog/2025/03/17/stilachirat-

analysis-from-system-reconnaissance-to-cryptocurrency-theft/ (last accessed: 17.05.2026).
[27] Binance. URL: https://www.binance.com/en (last accessed: 17.05.2026).
[28] Антонюк Н. О. Правова природа легітимаційного знаку. *Науковий вісник Львівського державного університету внутрішніх справ*. 2010. № 2. С. 278–285.
[29] Binance: Protect Your Crypto: Understanding the Ongoing Global Malware Attacks and What We Are Doing to Stop Them. URL: https://www.binance.com/en/blog/security/7968393135385409266 (last accessed: 17.05.2026).
[30] Tsuchiya T., Dong J.-D., Soska K., Christin N. Blockchain Address Poisoning. Proceedings of the 34th USENIX Security Symposium, Seattle, WA, USA, August 13-15, 2025. Seattle, 2025. P. 1243–1262. https://doi.org/10.48550/arXiv.2501.16681.
[31] Gao B., Wang H., Xia P., Wu S., Zhou Y., Luo X., Tyson G. Tracking Counterfeit Cryptocurrency End-to-end. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*. 2020. Vol. 4, issue 3. P. 50:1–50:28. https://doi.org/10.48550/arXiv.2011.02673.
[32] Майданик Р. Смарт-контракт криптоактивів у цивільному праві України. *Вісник Київського національного університету імені Тараса Шевченка*. 2024. № 1(127). С. 39–44. https://doi.org/10.17721/1728-2195/2024/1.127-7.
[33] Morrison R., Mazey N. C. H. L., Wingreen S. C. The DAO Controversy: The Case for a New Species of Corporate Governance?. *Frontiers in Blockchain*. 2020. Vol. 3. P. 25:1–25:13. https://doi.org/10.3389/fbloc.2020.00025.

References

[1] CoinGecko. (2025). *2025 Q3 Crypto Industry Report*. Retrieved from https://www.coingecko.com/research/publications/2025-q3-crypto-report.
[2] Dudorov, O.O., & Pysmenskyi, Ye.O. (Eds.). (2012). *Criminal law (Special part): Textbook* (Vol. 1). Luhansk: Elton-2.
[3] Antoniuk, N.O. (2012). *Criminal-law protection of property: Study guide*. Lviv: Ivan Franko National University of Lviv.
[4] Demidova, L. (2015). Incorporeal thing as the subject of a crime. *Bulletin of the National Academy of Legal Sciences of Ukraine, 2*(81), 101-108.
[5] Dorokhina, Yu.A. (2016). *Crimes against property. Theoretical and legal research*. Kyiv: Kyiv National University of Trade and Economics.
[6] Kryshevich, O., & Roshchyna, I. (2022). Cryptocurrency as a subject of a criminal offense against property: National and international law. *Bulletin of Mariupol State University. Series: Law*, *23-24*, 168-175. https://doi.org/10.34079/2226-3047-2022-12-23-24-168-175.
[7] Dumchykov, M.O. (2022). Features of the qualification of fraud in cyberspace, the means of committing which are virtual assets. *Scientific-Informational Bulletin of Ivano-Frankivsk University of Law named after King Danylo Halytskyi. Series: Law, 14*(26), 159–165. https://doi.org/10.33098/2078-6670.2022.14.26.149-155.
[8] Kozii, V. (2023). Criminal liability for illegal possession of cryptocurrency in Ukraine. *Social & Legal Studios, 6*(1), 33-40. https://doi.org/10.32518/sals1.2023.33.
[9] Shchehlakov, I.E. (2025). Problems of differentiating crypto-terms in the qualification of criminal offenses against property. *Bulletin of the Association of Criminal Law of Ukraine, 1*(23), 225-246. https://doi.org/10.21564/2311-9640.2025.23.331560.
[10] Ordekian, M., Atondo-Siu, G., Hutchings, A., & Vasek, M. (2024). Investigating wrench attacks: Physical attacks targeting cryptocurrency users. In *6th Conference*

on Advances in Financial Technologies (AFT 2024) (pp. 24:1–24:24). https://doi.org/10.4230/LIPIcs.AFT.2024.24.

[11] TRM Labs. (n.d.). *The rise of wrench attacks and crypto-related violent crime*. Retrieved from https://www.trmlabs.com/resources/blog/the-rise-of-wrench-attacks-and-crypto-related-violent-crime.

[12] *Verdict of the Obukhiv District Court of Kyiv Oblast in case No. 761/31532/21. (December 6, 2022)*. Retrieved from https://reyestr.court.gov.ua/Review/107735753.

[13] Kyiv City Prosecutor's Office. (n.d.). *Four pseudo-law enforcement officers detained in Kyiv for coercing a crypto-businessman to transfer 250 thousand US dollars under threats*. Retrieved from https://kyiv.gp.gov.ua/ua/news.html?_m=publications&_c=view&_t=rec&id=368660.

[14] *Verdict of the Obolonskyi District Court of the City of Kyiv in case No. 756/12186/24*. (December 10, 2024). Retrieved from https://reyestr.court.gov.ua/Review/123696369.

[15] *Verdict of the Saratskyi District Court of Odesa Oblast in case No. 513/1179/24*. (October 23, 2024). Retrieved from https://reyestr.court.gov.ua/Review/122489352.

[16] Tiwari, M., Lupton, C., Bernot, A., & Halteh, Kh. (2024). The cryptocurrency conundrum: The emerging role of digital currencies in geopolitical conflicts. *Journal of Financial Crime, 31*(6), 1622-1634. https://doi.org/10.1108/JFC-12-2023-0306.

[17] Watters, C. (2023). When criminals abuse the blockchain: Establishing personal jurisdiction in a decentralised environment. *Laws, 12*(2), 1-16. https://doi.org/10.3390/laws12020033.

[18] U.S. Department of Justice. (n.d.). *BitConnect founder indicted in global $2.4 billion cryptocurrency scheme*. Retrieved from https://www.justice.gov/archives/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme.

[19] Maras, M.-H., & Ives, E.R. (2024). Deconstructing a form of hybrid investment fraud: Examining 'pig butchering' in the United States. *Journal of Economic Criminology, 5*(3), 1-19. https://doi.org/10.1016/j.jeconc.2024.100066.

[20] The Department of Financial Protection and Innovation. (n.d.). *Pig butchering – how to spot and report the scam*. Retrieved from https://dfpi.ca.gov/news/insights/pig-butchering-how-to-spot-and-report-the-scam/.

[21] Shchehlakov, I.E. (May 21, 2025). Philosophical and legal problems of cryptocurrency decentralization. In *Philosophy and Law: Abstracts of the International scient. conf. of postgraduate students and students* (pp. 128-130). Kharkiv.

[22] United States Attorney's Office, Southern District of New York. (n.d.). *Southern District of New York: Samuel Bankman-Fried Sentenced to 25 Years in Prison*. Retrieved from https://www.justice.gov/usao-sdny/pr/samuel-bankman-fried-sentenced-25-years-prison.

[23] Mackenzie, S. (2025). Crypto collapse: The cult of personality and the normalisation of fraud in FTX and Celsius. *Journal of Financial Crime, 32*(6), 288-303. https://doi.org/10.1108/JFC-01-2024-0054.

[24] *Law of Ukraine No. 2074-IX "On Virtual Assets"*. (February 17, 2022). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20.

[25] Singh, A., Choudhary, P., Singh, A.K., & Tyagi, D.K. (2021). Keylogger detection and prevention. *Journal of Physics: Conference Series, 2007*(1), 1-8. https://doi.org/10.1088/1742-6596/2007/1/012005.

[26] Microsoft. (2025). *StilachiRAT analysis: From system reconnaissance to cryptocurrency theft*. Retrieved from https://www.microsoft.com/en-us/security/blog/2025/03/17/stilachirat-analysis-from-system-reconnaissance-to-cryptocurrency-theft/.

[27] *Binance*. (n.d.). Retrieved from https://www.binance.com/en.
[28] Antoniuk, N.O. (2010). Legal nature of the legitimation sign. *Scientific Bulletin of Lviv State University of Internal Affairs*, *2*, 278-285.
[29] Binance. (n.d.). *Protect your crypto: Understanding the ongoing global malware attacks and what we are doing to stop them*. Retrieved from https://www.binance.com/en/blog/security/7968393135385409266.
[30] Tsuchiya, T., Dong, J.-D., Soska, K., & Christin, N. (August 13-15, 2025). Blockchain address poisoning. In *Proceedings of the 34th USENIX Security Symposium* (pp. 1243-1262). Seattle, WA, USA. https://doi.org/10.48550/arXiv.2501.16681.
[31] Gao, B., Wang, H., Xia, P., Wu, S., Zhou, Y., Luo, X., & Tyson, G. (2020). Tracking counterfeit cryptocurrency end-to-end. *Proceedings of the ACM on Measurement and Analysis of Computing Systems, 4*(3), 50:1-50:28. https://doi.org/10.48550/arXiv.2011.02673.
[32] Maidanyk, R. (2024). Smart contract on cryptoassets in the civil law of Ukraine. *Bulletin of Taras Shevchenko National University of Kyiv, 1*(127), 39-44. https://doi.org/10.17721/1728-2195/2024/1.127-7.
[33] Morrison, R., Mazey, N.C.H.L., & Wingreen, S.C. (2020). The DAO controversy: The case for a new species of corporate governance? *Frontiers in Blockchain, 3,* 1-13. https://doi.org/10.3389/fbloc.2020.00025.

Іван Едуардович Щеглаков
аспірант кафедри кримінально-правової політики
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Григорія Сковороди, 77, Харків, Україна
e-mail: shived1@ukr.net
ORCID 0009-0001-5042-072X

Ivan E. Shchehlakov
Ph.D. Student at the Department of Criminal Law Policy
Yaroslav Mudryi National Law University
61024, 77 Hryhoriia Skovorody Str., Kharkiv, Ukraine
e-mail: shived1@ukr.net
ORCID 0009-0001-5042-072X

Рекомендоване цитування: Щеглаков І. Е. Способи посягання на криптовласність: основні види та кваліфікація. *Проблеми законності*. 2026. Вип. 173. С. 304–330. https://doi.org/10.21564/2414-990X.173.361496.

Suggested Citation: Shchehlakov, I.E. (2026). Methods of Encroachment on Cryptoproperty: Main Types and Qualification. *Problems of Legality, 173*, 304-330. https://doi.org/10.21564/2414-990X.173.361496.

Статтю подано / Submitted: 05.04.2026
Доопрацьовано / Revised: 05.05.2026
Схвалено до друку / Accepted: 28.05.2026
Опубліковано / Published: 29.05.2026