УДК 343.53:343.72:339.19:336.74
DOI https://doi.org/10.24144/2307-3322.2024.86.5.16

ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ ШАХРАЙСТВА, ПОВ'ЯЗАНОГО З ВИКОРИСТАННЯМ КРИПТОАКТИВІВ

Неганов В.В.,
кандидат юридичних наук,
старший науковий співробітник наукової лабораторії
з проблем протидії злочинності ННІ № 1
Національної академії внутрішніх справ
ORCID: 0000-0002-1430-8343

Мамка Г.М.,
доктор юридичних наук,
заступник голови Комітету
з питань правоохоронної діяльності
Верховної Ради України
ORCID: 0000-0002-2918-4777

Крижевський А.В.,
кандидат юридичних наук, докторант
Національної академії внутрішніх справ
ORCID: 0009-0001-9646-1359

Неганов В.В., Мамка Г.М., Крижевський А.В. Особливості кваліфікації шахрайства, пов'язаного з використанням криптоактивів.

У публікації розглянуто питання підстав кримінальної відповідальності за шахрайство за ст. 190 Кримінального кодексу України. Окреслено особливості кваліфікації, що містяться, зокрема, у четвертій частині зазначеної статті стосовно незаконних операцій з використанням електронно-обчислювальної техніки і п'ятій частині стосовно шахрайства, вчиненого організованою групою. Акцентовано, що в національному законодавстві немає чіткого визначення поняття «електронно-обчислювальна техніка» та зазначено, що використання законодавцем даного терміна в тексті статті не цілком відповідає принципу юридичної визначеності.

Виокремлено кримінально-правові ознаки шахрайства, пов'язаного з використанням криптоактивів шляхом незаконних операцій, здійснених за допомогою електронно-обчислювальної техніки, і шахрайства, пов'язаного з використанням криптоактивів, учиненого організованою групою.

Досліджено типову організацію злочину з деталізованим розподілом ролей співучасників шахрайства, пов'язаного з використанням криптоактивів. Визначено додаткові ознаки організованого злочинного угруповання, яке вчиняє шахрайства, пов'язані з використанням криптоактивів, зокрема тривалість діяльності злочинного угруповання; наявність спеціалізації в діяльності злочинного угруповання; наявність лідера з владними повноваженнями; розподіл функціональних обов'язків серед членів угруповання; корислива спрямованість злочинної діяльності групи; створення системи захисту від викриття. На підставі аналізу судових рішень наведено приклади таких дій.

Найпоширенішим видом шахрайств, пов'язаних з використанням криптоактивів в Україні, 2024 року визнані шахрайства, вчинені з використанням міжнародних криптовалютних бірж (наприклад Binance).

Ключові слова: шахрайство, криптоактиви, організована група, організоване злочинне угруповання, кримінальна відповідальність.

Nehanov V.V., Mamka H.M., Kryzhevskyi A.V. Features of qualification of fraud related to the use of cryptoassets.

Manuscript presents the genesis regarding the grounds for criminal liability for fraud: Art. 190 of the Criminal Code of Ukraine. The features of the qualification contained, in particular, in the fourth part of the article regarding illegal operations with using electronic computing equipment and the fifth part of the article regarding fraud committed by an organized group. It is emphasized that the national legislation does not have a clear definition of the concept of «electronic and computing equipment» and it is noted that the legislator's use of this term in the text of the article does not fully comply with the principle of legal certainty.

The criminal-legal features of fraud associated with the use of cryptoassets through illegal operations using electronic computing equipment and fraud associated with the use of cryptoassets committed by an organized group are determined.

A typical organization of the crime is described with a detailed distribution of the roles of accomplices in fraud associated with the use of cryptoassets. Additional features of an organized criminal group that commits fraud associated with the use of cryptoassets are outlined, in particular, the duration of the criminal group's activities; the presence of specialization in the activities of the criminal group; the presence of a leader with authority; the distribution of functional responsibilities among the members of the group; the self-serving orientation of the group's criminal activities; the creation of a system of protection against exposure. Examples of such actions contained in the decisions of Ukrainian courts are given.

The most common type of fraud involving the use of crypto assets in Ukraine in 2024 was fraud committed using international cryptocurrency exchanges (for example, Binance).

Key words: fraud, cryptoassets, organized criminal group, criminal liability.

Постановка проблеми. У сучасному світі технологічний прогрес суттєво випереджає процес внесення змін до національного законодавства, що мають регулювати сферу їхнього застосування. Для того щоб на належному рівні забезпечувати правопорядок у цій сфері, кримінально-правові засоби необхідно своєчасно та якісно оновлювати, з огляду на висновки й узагальнення судової та слідчої практики.

Стрімкий розвиток економіки й цифрових технологій зумовив появу нової групи об'єктів – «віртуальних активів». Криптоактиви не мають матеріальної форми та самостійної майнової цінності, їх створюють за допомогою інформаційних технологій та блокчейн-системи тощо [1]. Згідно з даними TripleA, близько 6,5 млн українців, або понад 14 % від загальної кількості населення, мають у власності крипто активи [2]. Це посилює інтерес до використання криптоактивів у злочинній діяльності з боку представників організованої злочинності, які своєю чергою також «осучаснюють» форми й методи злочинних посягань на майно громадян. Зокрема, у звіті Департаменту кіберполіції Національної поліції України зазначено, що шахраї вигадують різноманітні схеми, серед яких: фейкові магазини, обманні пропозиції надання послуг щодо евакуації з небезпечних регіонів, фальшиве волонтерство, збори коштів для визволення військових з полону тощо [3]. Під час реалізації таких шахрайських схем кошти потерпілих громадян можуть надходити на рахунки третіх осіб, які виконують роль контрагентів шахраїв за криптобіржовими угодами.

За таких умов правоохоронні органи мають своєчасно вдосконалювати науково-практичну й методичну базу, ураховувати в оперативній та слідчій діяльності позицію судів, передусім Верховного Суду, під час розгляду відповідної категорії справ.

Стан опрацювання проблематики. Проблемні аспекти розслідування та кваліфікації шахрайства з використанням електронно-обчислювальної техніки досліджували такі науковці: Д. Азаров, О. Брисковська, А. Савченко, О. Самойленко, Р. Усманов, С. Чернявський, С. Чучко, А. Шевчишен та ін.

Мета статті – дослідити особливості кваліфікації та кримінально-правові ознаки шахрайства, пов'язаного з використанням криптоактивів шляхом незаконних операцій, здійснених за допомогою електронно-обчислювальної техніки, і шахрайства, пов'язаного з використанням криптоактивів, вчиненого організованою групою.

Виклад основного матеріалу. З 2001 року, коли набрав чинності новий Кримінальний кодекс України, кримінальна відповідальність за шахрайство зазнала змін, їх додатково вносили 2008-го, 2018-го та двічі 2023 року. Останні зміни до ст. 190 КК України були пов'язані з посиленням

кримінальної відповідальності. 2018 року внесено зміни в абзац другий частини першої ст. 190, зокрема слова «до п'ятдесяти» замінено словами «від двох тисяч до трьох тисяч», а після слів «громадськими роботами на строк» текст доповнено словами «від двохсот»; в абзаці другому частини другої слова «від п'ятдесяти до ста» замінено словами «від трьох тисяч до чотирьох тисяч» [4]. Такі зміни були пов'язані з необхідністю законодавчого врегулювання застосування положень КПК України стосовно особливостей досудового розслідування кримінальних проступків та їх судового розгляду. 2023 року було визначено нову редакцію ст. 190 «Шахрайство», у якій передбачено нову кваліфікуючу ознаку: «вчинене в умовах воєнного або надзвичайного стану» [5]. На цій проблемі неодноразово зосереджували увагу знані вчені [6–8]. Наступними змінами санкцію частини першої ст. 190 КК України доповнено новим видом кримінального покарання – пробаційним наглядом [9].

З огляду на дію воєнного стану в державі, а також обставини участі здебільшого декількох співучасників під час учинення шахрайства з використанням електронно-обчислювальної техніки, у зв'язку з прийняттям зазначених вище новел до ст. 190 КК України актуальним постає питання правильної кваліфікації цього кримінального правопорушення. Поняття «кваліфікація злочину» позначає процес встановлення відповідності між юридично значущими ознаками злочину (фактичний склад злочину) й ознаками злочину, передбаченими КК (юридичний склад злочину), а також формулювання висновку про наявність чи відсутність такої відповідності [10, с. 21].

Найпоширенішим видом шахрайств, пов'язаних з використанням криптоактивів в Україні, 2024 року є шахрайства, вчинені з використанням міжнародних криптовалютних бірж (наприклад Binance), які дають змогу проводити P2P (person-to-person) платіжні операції, коли одна сторона (продавець) продає віртуальні криптоактиви (BTC, Ethereum, USDT), а інша сторона (покупець) їх отримує на віртуальний криптогаманець і сплачує за це продавцю в національній валюті за банківськими реквізитами, що зазначені продавцем в ордері (заявці) замовлення. Подія шахрайства супроводжується переважно обставинами, коли покупець – суб'єкт кримінального правопорушення сплачує за криптоактив не власним коштом із власного рахунку, а з використовуючи банківські (карткові) рахунки третіх осіб, які формально не є сторонами біржової P2P угоди. У цьому випадку потерпілі – треті особи не знають про наявність відповідної біржової угоди, а переказують кошти за не відомими для них реквізитами за умовлянням особи (осіб) шахрая за вигадані товари, послуги, допомогу другу тощо. Унаслідок цього шахрай (хоча за цією схемою «працює» здебільшого не одна особа, а організована група) отримує на контрольований ним віртуальний гаманець (часто оформлений на «дропа» –підставну особу) криптоактив, який згодом у певний спосіб переводять у фіатні гроші, наприклад, у гривню.

Оскільки безпосереднім об'єктом шахрайства, пов'язаного з використанням криптоактивів, стає здебільшого приватна власність, а предметом злочину – безготівкові грошові кошти, для забезпечення правильної кваліфікації кримінального правопорушення сума збитків, яких завдають потерпілій особі, має співвідноситися (відповідати) юридичному складу інкримінованої частини ст. 190 КК України.

Стаття 51 КУпАП встановлює адміністративну відповідальність за дрібне викрадення чужого майна шляхом крадіжки, шахрайства, привласнення чи розтрати. Частиною другою цієї статті в новій редакції (Закон України від 18 липня 2024 року № 3886-IX) встановлено верхній поріг вартості викраденого майна в розмірі двох неоподатковуваних мінімумів доходів громадян (2024 року це 3028 грн). Отже, кримінальна відповідальність за ст. 190 КК України настає за заволодіння чужого майна вартістю понад два неоподатковувані мінімуми доходів громадян. На нашу думку, будь-які дії, що були пов'язані із заволодінням шляхом обману грошовими (безготівковими) коштами потерпілої особи, зокрема шляхом незаконних операцій з використанням електронно-обчислювальної техніки, у сумі, що не перевищує 2 НМДГ, не можна кваліфікувати за статтею Особливої частини КК України.

До (особливо) кваліфікуючих ознак шахрайства, які мають інтерес у контексті цієї роботи, зосередимо увагу на ознаках, що містяться в четвертій та п'ятій частинах ст. 190 КК України. Якщо слідчий шляхом з'ясування відповідних обставин у кримінальному провадженні достовірно встановить наявність або відсутність таких (особливо) кваліфікуючих ознак, як спосіб обману, розмір завданої шкоди, форма співучасті, це надає можливість органу досудового розслідування правильно кваліфікувати відповідний злочин, а отже, і забезпечувати виконання завдань кримінального провадження.

У випадку шахрайства з використанням криптоактивів і мережі міжнародних криптовалютних бірж, а також наявності обставин заволодіння чужого майна вартістю понад два НМДГ може бути встановлено наявність кваліфікуючих ознак, передбачених ч. 4 ст. 190 КК України: заволодіння чужим майном у великому розмірі або шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки.

Розглядаючи специфічний спосіб обману, слід зауважити, що в національному законодавстві немає чіткого визначення поняття «електронно-обчислювальна техніка». Натомість у ст. 361-2, 362, 363, 363-1 КК України міститься поняття «електронно-обчислювальна машина (комп'ютер)» (ЕОМ). Стрімкий розвиток цифрової обчислювальної техніки й становлення науки про принципи її побудови та проєктування розпочалися в 40-х роках ХХ ст., коли технічною базою стала електроніка, згодом – мікроелектроніка, а основою для розвитку архітектури комп'ютерів (електронних обчислювальних машин, ЕОМ) – досягнення в галузі штучного інтелекту [11]. Отже, поняття «електронно-обчислювальна техніка» є ширшим і має охоплювати ЕОМ.

Визначення цього поняття містять відомчі акти (накази) деяких органів центральної виконавчої влади. Зокрема, згідно з Наказом Міністерства доходів і зборів України від 05.09.2013 № 443, електронно-обчислювальна машина (ЕОМ) – електронно-обчислювальна машина з необов'язковими додатковими пристроями, системними елементами (пристрої для друку, сканери, модеми, блоки безперервного живлення та інші спеціальні периферійні пристрої); периферійні пристрої – сукупність необов'язкових додаткових пристроїв, які використовуються в процесі діяльності оператора ЕОМ (клавіатура, маніпулятор «миша», дискова система, звукова система, модем, мікрофон, принтер, сканер тощо) [12].

Науковці критично ставляться до визначення такого способу обману, як «з використанням електронно-обчислювальної техніки», у ст. 190 КК України. Зокрема, Д. Азаров пропонує виключити фразу «або шляхом незаконних операцій з використанням електронно-обчислювальної техніки» з тексту статті, оскільки, на його думку, такі дії цілком охоплені незаконним втручанням у процес обробки комп'ютерної інформації, учиненим із корисливих мотивів [13, с. 14]. А. Савченко вважає, що шахрайство в цьому випадку полягає у введенні до електронно-обчислювальних машин (комп'ютера), автоматизованої системи, комп'ютерної мережі чи мережі електрозв'язку неправдивих відомостей (особа, отримавши доступ до автоматизованої системи банківської установи, вводить або змінює комп'ютерну інформацію, унаслідок чого грошові кошти переводять з рахунку потерпілого на інший рахунок), а відповідні захисні (охоронні) системи чи комп'ютерні програми сприймають зазначені неправдиві відомості як такі, що здійснені за власним бажанням потерпілого чи за його особистим дорученням [14].

На наше переконання, специфічний спосіб обману, визначений у ч. 4 ст. 190 КК України, може поширюватися на незаконні операції з використанням, зокрема, комп'ютерів, ноутбуків, планшетів, смартфонів та іншої сучасної цифрової техніки, проте використання законодавцем терміна «електронно-обчислювальна техніка» в тексті статті справді не цілком відповідає принципу юридичної визначеності.

Також слід розглянути, які саме операції з використанням комп'ютерів, ноутбуків, планшетів, смартфонів та іншої сучасної цифрової техніки можна кваліфікувати як незаконні, оскільки лише їх може бути використано як спосіб обману за цією частиною статті. На нашу думку, лише використання ЕОМ під час шахрайських дій не утворює спеціальну кваліфікуючу ознаку шахрайства. Схожу позицію висловлено в постанові Верховного Суду від 4 липня 2024 року, справа № 752/8994/22: *«Апеляційний суд, відхиляючи доводи захисту, вдався до тлумачення поняття електронно-обчислювальної машини (ЕОМ) та формально вказав, що суд першої інстанції дійшов правильного переконання про необхідність кваліфікації дій винного за ч. 3 ст. 190 КК України тому, що знаряддям вчинення злочину засуджений використав Айфон 6+.*

Однак суд апеляційної інстанції залишив поза увагою те, що саме по собі використання ЕОМ для неправомірного заволодіння чужим майном без здійснення з її використанням незаконних операцій шляхом обману чи зловживання довірою не утворюють складу вказаного кваліфікованого виду шахрайства. Стала судова практика зводиться до того, що використання ЕОМ без здійснення незаконних операцій з її використанням, шляхом обману чи зловживання довірою, не утворює спеціальну кваліфікуючу ознаку шахрайства "вчинення шляхом незаконних операцій з використанням електронно-обчислювальної техніки" (до прикладу постанови ВС у справах № 750/6192/17, № 159/2149/17,№607/9095/22, № 484/1701/20)… У даному кримінальному про-

вадженні судами не встановлено, що ОСОБА_7 з використанням мережі електрозв`язку (мобільного телефону) здійснював незаконні операції, спрямовані на заволодіння грошима потерпілої. Фактично використання ОСОБА_7 мобільного телефона полягало лише в спілкуванні з ОСОБА_8 у месенджері Telegram, під час якого засуджений повідомив потерпілій неправдиві відомості про надання ним послуги перевезення її матері з м. Маріуполь, де проходили бойові дії, у безпечне місце, та в подальшому отримав на вказану ним банківську карту гроші потерпілої, які вона перераховувала самостійно, добровільно, у легальний спосіб з використанням інтернет-банкінгу» [15].

Показовими є метадані, які наводить у своїй роботі Р. Усманов. За результатами метадослідження 438 судових рішень категорії «продаж товарів» (щодо продажу товарів через спеціалізовані інтернет-майданчики за умови відсутності таких товарів і з метою привласнити передплату), виявлено прогресивну динаміку зменшення відсотка судових рішень, у яких дії винних осіб отримували кримінально-правову оцінку національними судами як шахрайство, вчинене шляхом незаконних операцій з використанням комп'ютерної техніки: з 85 % 2011 року до 50 % 2023 року [16]. З огляду на зазначену вище позицію Верховного Суду, яку мають ураховувати суди першої та апеляційної інстанцій, така динаміка щодо кваліфікації у справах відповідної категорії, за умови відсутності відповідних змін у кримінальному законодавстві, буде лише посилюватися.

У випадку вчинення шахрайства з використанням міжнародних криптовалютних бірж шахраї здійснюють нелегітимні (неправомірні) за угодами (правилами) діяльності P2P біржі дії щодо: створення (прийняття) заявки з метою передання даних про картковий рахунок для здійснення оплати третій сторонній особі (потерпілому в кримінальному провадженні), отримання криптоактива на підставі сплати ордера від третьої особи, використання документів і паспортних даних підставних осіб для реєстрації торговельного акаунту на біржі (з метою приховування справжньої особи злочинця у випадку звернення правоохоронних органів до криптобіржі) тощо.

Усі ці незаконні дії з використанням ЕОМ здійснюють шахраї для забезпечення анонімності, приховування слідів злочину. Тому під час кваліфікації за ч. 4 в цій категорії злочинів необов'язковим стає доведення обставин заволодіння чужого майна у великих розмірах (понад 250 НМДГ), оскільки кваліфікована ознака злочину переважно вже наявна.

Якщо вчинено заволодіння чужим майном в особливо великих розмірах (понад 600 НМДГ) або організованою групою, кваліфікуюча ознака щодо способу обману не має такого визначального значення і відповідні шахрайства з використанням криптоактивів слід кваліфікувати за ч. 5 ст. 190 КК України.

Відповідно до ч. 3 ст. 28 КК України, злочин визнають учиненим організованою групою, якщо в його готуванні або вчиненні брали участь три і більше осіб, які попередньо зорганізувалися в стійке об'єднання для вчинення цього та іншого (інших) кримінальних правопорушень, об'єднаних єдиним планом з розподілом функцій учасників групи, спрямованих на досягнення цього плану, відомого всім учасникам групи. Оскільки організована група осіб передбачає розподіл функцій і ролей, то в злочині повинні брати участь, крім виконавців, інші учасники в ролі організаторів, підбурювачів та пособників. Отже, злочин, учинений трьома учасниками організованої групи, з яких лише один був виконавцем, слід визнавати учиненим організованою групою. Безпосередньо виконувати об'єктивну сторону злочину може й одна особа в ролі виконавця [17]. Крім основних (обов'язкових) ознак організованих груп, які перелічено в ст. 28 КК України, науковці визначають і додаткові (факультативні) ознаки, про деякі з них буде зазначено нижче.

Під час учинення шахрайства, пов'язаного з використанням криптоактивів, типовою є така організація злочину:

– виконавець шляхом обману або зловживання довірою переважно за допомогою телефонних дзвінків, листування в месенджерах (Viber, Telegram) умовляє потерпілу особу перевести банківським переказом (як сплату за вигадані товари, послуги тощо) власні кошти на банківський (картковий) рахунок особи, яка не входить до складу організованого злочинного угруповання і легітимно розмістила P2P заявку на продаж криптоактива на криптобіржі;

– співвиконавець або пособник заздалегідь передає виконавцю дані, отримані на криптобіржі, про банківський рахунок (карту), на яку потерпіла особа має переказати кошти;

– інший пособник підшукує потенційних потерпілих у мережі Інтернет шляхом створення або перегляду (з подальшим переданням контактних даних потенційної потерпілої особи виконавцю) оголошень, повідомлень у соціальних мережах, роздрібних торговельних майданчиків про вигадані товари, послуги;

– організатор здійснює координацію, керування злочинною групою, контролює подальший розподіл грошових коштів, які шляхом обману або зловживання довірою було отримано від потерпілої особи. Водночас може бути суміщено роль організатора з пособником або співвиконавцем такого злочину.

Слід виокремити додаткові ознаки організованого злочинного угруповання, яке вчиняє шахрайства, пов'язані з використанням криптоактивів:

– тривалість діяльності злочинного угруповання: через технологічну складність і тривалість налагодження цифрової та комунікаційної інфраструктури, яка має сприяти вчиненню злочинною групою відповідного шахрайства, немає практичного сенсу з позицій «витрати/прибутки» здійснювати незначну кількість епізодів відповідного шахрайства;

– наявність спеціалізації в діяльності злочинного угруповання: окреслений вище типовий розподіл ролей у співучасті обумовлює відповідну спеціалізацію;

– наявність лідера з владними повноваженнями – організатора;

– розподіл функціональних обов'язків серед членів угруповання обумовлений, зокрема, необхідністю використання спеціальних технічних знань у сфері криптоактивів;

– корислива спрямованість злочинної діяльності групи обумовлена об'єктивною стороною кримінального правопорушення;

– створення системи захисту від викриття: використання документів дропів (підставних осіб) з метою реєстрації акаунтів на міжнародних криптобіржах, відкриття банківських рахунків.

За результатами емпіричного аналізу судових вироків, що містяться у відкритому доступі в Єдиному державному реєстрі судових рішень, виявлено лише сім вироків, у тексті яких одночасно містяться такі ключові слова: «шахрайство», «організованою групою», «криптовалюта». Та сама пошукова комбінація, але з використанням терміна «криптоактив», не видає жодних результатів. Це дає підстави стверджувати, що як органи досудового розслідування, так і національні суди у своїх рішеннях не цілком правильно використовують понятійний апарат. Поняттям «криптовалюта» послуговуються не завжди доречно, оскільки корінь «валют» вказує на категорію «валюта», а криптоактиви не є валютою за чинним законодавством. Крім того, з огляду на високу мінливість цін, обмеженість сфери обігу й відсутність свободи в їх використанні як засобів платежу, криптографічні цінності не можна віднести до грошей, а лише до активів, що спонукає використовувати термін «криптоактиви», який не містить такої суперечності [18].

Прикладом шахрайства, пов'язаного з використанням криптоактивів, учиненого організованим злочинним угрупованням, є деякі обставини з вирокуБерезанського районного суду Миколаївської області від 28 липня 2023 року у справі № 469/1053/23, яким затверджено угоду про визнання винуватості (загалом за вироком встановлено дев'ять епізодів учинення шахрайства, пов'язаного з використанням криптоактивів (USDT) обвинуваченою особою в складі організованого злочинного угруповання):

«Особою, судовий розгляд щодо якої у кримінальному провадженні № 12022150000000209 від 25 серпня 2022 року здійснюється в іншому судовому провадженні, ***як організатором злочинної групи****, були визначені функції ОСОБА_5, ОСОБА_4, ОСОБА_6 та не встановленої в ході досудового розслідування особи, що складалися з дій, спрямованих на досягнення єдиного злочинного результату, а саме заволодіння грошовими коштами ПАТ "БАНК ВОСТОК", які полягали в такому:*

– несанкціоноване втручання не встановленою в ході досудового розслідування особою в роботу автоматизованої системи – міжнародної платіжної системи "MasterCard", що призведе до підробки інформації, а саме створення фіктивних транзакцій від торгової точки BuckeyeConcretePumping OH Middletown USA, який ініціював повернення грошових коштів, що не належать клієнту, на його картку;

– пошук осіб для використання їх даних для відкриття банківських рахунків в ПАТ "БАНК ВОСТОК"з метою надання реквізитів вказаних банківських рахунків для створення фіктивних транзакцій;

– контроль за банківськими рахунками вищевказаних осіб шляхом отримання логіну та паролю для входу в акаунт банкінгу;

– з використанням власних акаунтів на криптовалютній біржі "Binance" пошук ордерів послуги «P2P» (тобто грошові перекази з банківського рахунку покупця на банківський рахунок продавця, у результаті яких покупець отримує криптовалюту на свій фінансовий рахунок криптовалютної біржі) на максимальні суми (30 000 грн) на криптовалютній біржі "Binance" для по-

дальшого швидкого перерахунку грошових коштів з банківських рахунків ПАТ "БАНК ВОСТОК", на які помилково були зараховані грошові кошти в результаті фіктивної транзакції;

– безпосередня купівля криптовалюти USDT шляхом перерахунку грошових коштів з вищевказаних банківських рахунків на банківські рахунки продавців P2P на криптовалютній біржі "Binance";

– перерахунок криптовалюти USDT з кастодіального гаманця власних акаунтів криптовалютної біржі "Binance" на кастодіальний гаманець, наданий особою, судовий розгляд щодо якої в кримінальному провадженні № 12022150000000209 від 25 серпня 2022 року здійснюється в іншому судовому провадженні.

Зорганізувавшись таким чином у стійке злочинне об'єднання, реалізуючи свій спільний злочинний умисел, діючи відповідно до розробленого особою, судовий розгляд щодо якої в кримінальному провадженні № 12022150000000209 від 25 серпня 2022 року здійснюється в іншому судовому провадженні, плану вчинення злочину, на початку серпня 2022 року, точна дата та час досудовим слідством не встановлені, ОСОБА_5, ОСОБА_4 та ОСОБА_6 підшукали ОСОБА_10, ОСОБА_11, ОСОБА_12, ОСОБА_13, ОСОБА_14, ОСОБА_15, ОСОБА_16, ОСОБА_17, ОСОБА_18, ОСОБА_19, ОСОБА_20, ОСОБА_21 та ОСОБА_22, які за вказівкою ОСОБА_5, ОСОБА_4 та ОСОБА_6 відкрили банківські рахунки в ПАТ "БАНК ВОСТОК", встановивши та авторизувавшись через додаток "Дія" в мобільному банкінгу "Банк власний рахунок", і передали логіни та паролі для входу в акаунти ОСОБА_5, ОСОБА_4 та ОСОБА_6, у результаті чого ОСОБА_5, ОСОБА_4 та ОСОБА_6 отримали можливість розпоряджатися грошовими коштами, які акумулювалися на вказаних банківських рахунках…

У результаті вказаних протиправних дій 06 серпня 2022 року ОСОБА_5 з особою, судовий розгляд щодо якої в кримінальному провадженні № 12022150000000209 від 25 серпня 2022 року здійснюється в іншому судовому провадженні, діючи в складі організованої групи, в результаті підробки невстановленою особою, матеріали відносно якої виділені в окреме провадження, у невстановлений спосіб транзакції "refund" в ПАТ "Банк ВОСТОК", шляхом обману заволоділи грошовими коштами ПАТ "Банк ВОСТОК" на суму 23 800 грн, у результаті чого спричинили ПАТ "Банк ВОСТОК" матеріальні збитки на вказану суму…

У результаті вказаних протиправних дій 06 серпня 2022 року ОСОБА_5 з особою, судовий розгляд щодо якої в кримінальному провадженні № 12022150000000209 від 25 серпня 2022 року здійснюється в іншому судовому провадженні, діючи у складі організованої групи, в результаті підробки невстановленою особою, матеріали відносно якої виділені в окреме провадження, у невстановлений спосіб транзакції "refund" в ПАТ "Банк ВОСТОК" шляхом обману заволоділи грошовими коштами на суму 98 716,51 грн, в результаті чого спричинили ПАТ "Банк ВОСТОК" матеріальні збитки на вказану суму» [19].

Висновки. За результатами здійсненого дослідження визначено особливості правильної кваліфікації шахрайств, пов'язаних з використанням криптоактивів, проаналізовано відповідну судову практику й авторські рекомендації, які можуть використовувати органи досудового розслідування. Зокрема, увагу зосереджено на формулюванні специфічного способу обману, визначеного в ч. 4 ст. 190 КК України, що не цілком відповідає принципу юридичної визначеності.

Розглянута типова організація злочину з деталізованим розподілом ролей співучасників шахрайства, пов'язаного з використанням криптоактивів, засвідчує, що забезпечення реалізації таких шахрайських схем відбувається переважно за участю організованого злочинного угруповання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ерастов В., Гудзь Г. Ринок криптоактивів в Україні: тенденції сучасності *Економіка та суспільство*. 2023. № 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-1.
2. Global Cryptocurrency Ownership Data 2023. URL: https://triple-a.io/crypto-own-ership-data.
3. Онлайн-шахрайство під час війни: як захистити себе від фінансових втрат. URL: https://sud.ua/uk/news/ukraine/299885-onlayn-moshennichestvo-vo-vremya-voyny-kak-zaschititsebya-ot-finansovykh-poter.
4. Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень : Закон України від 22 листоп. 2018 р. № 2617-VIII. URL: https://zakon.rada.gov.ua/laws/show/2617-19.

5. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо усунення суперечностей у караності кримінальних правопорушень : Закон України від 13 лип. 2023 р. № 3233-IX. URL: https://zakon.rada.gov.ua/laws/show/3233-20.
6. Вознюк А.А. Воєнний або надзвичайний стан як обставина, що впливає на кваліфікацію кримінального правопорушення або призначення покарання: актуальні питання вдосконалення кримінального законодавства. *Проблеми кваліфікації та розслідування кримінальних правопорушень в умовах воєнного стану*: матеріали наук.-теорет. конф. (Київ, 26 трав. 2022 р.). Київ: Нац. акад. внутр. справ, 2022. С. 43–54.
7. Вознюк А.А. Воєнний та надзвичайний стан як обставини, що впливають на кваліфікацію кримінального правопорушення або призначення покарання. *Юридичний науковий електронний журнал*. 2022. № 6. С. 308–317. DOI: https://doi.org/10.32782/2524-0374/2022-6/69.
8. Новели кримінального законодавства України, прийняті в умовах воєнного стану: наук.-практ. комент. / А.А. Вознюк, О.О. Дудоров, Р.О. Мовчан та ін.; за ред. А.А. Вознюка, Р.О. Мовчана, В.В. Чернєя. Київ : Норма права, 2022. 278 с.
9. Про внесення змін до Кримінального, Кримінального процесуального кодексів України та інших законодавчих актів України щодо удосконалення видів кримінальних покарань: Закон України від 23 серп. 2023 р. № 3342-IX. URL: https://zakon.rada.gov.ua/ laws/show/3342-20.
10. Кузнецов В.В., Савченко А.В. Теорія кваліфікації злочинів : підручник / за заг. ред. Є.М. Моісеєва, О.М. Джужі. Київ: ПАЛИВОДА А.В., 2006. 300 с.
11. Історія та розвиток комп'ютерної техніки та обчислювальних машин / за матеріалами книг Б.М. Малиновського. URL: http://www.icfcst.kiev.ua/MUSEUM/ Early_u.html.
12. Про затвердження Примірної інструкції з охорони праці під час експлуатації електронно-обчислювальних машин : наказ Міністерства доходів і зборів України від 05.09.2013 № 443. URL: https://zakon.rada.gov.ua/ rada/show/v0443810-13.
13. Азаров Д.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: автореф. дис. ... канд. юрид. наук: 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». Київ, 2003. 18 с.
14. Савченко А.В. Щодо удосконалення кваліфікуючих та особливо кваліфікуючих ознак шахрайства. *Теоретичні та прикладні проблеми кримінального права України*: матер. Міжнар. наук.-практ. конф. (Луганськ, 20–21 трав. 2011 р.). 2011. С. 417–422.
15. Постанова Верховного Суду від 04 лип. 2024 р. у справі № 752/8994/22. URL: http://iplex.com.ua/doc.php?regnum=120244099&red= 1000030c361919f7038a229e34b5ef4aebcfbb&d=5.
16. Усманов Р. Шахрайство з використанням електронно-обчислювальної техніки: аналіз судової практики. *Науковий вісник Львівського державного університету внутрішніх справ*. 2024. № 1. С. 153–163.
17. Вознюк А.А. Кількісно-якісний склад учасників організованої групи. *Кримінологічна теорія і практика: досвід, проблеми сьогодення та шляхи їх вирішення* : тези доп. наук.-теорет. конф. (Київ, 20 берез. 2014 р.). Київ: Нац. акад. внутр. справ, 2014. С. 231–234.
18. Тригуб О., Пасевич Д. Міжнародний досвід створення системи регулювання ринку криптоактивів. *Регулювання та перспективи ринку криптоактивів* : зб. матеріалів наук. форуму КНЕУ ім. Вадима Гетьмана. Київ, 2018. С. 86–89
19. Вирок Березанського районного суду Миколаївської області від 28 лип. 2023 р. Справа № 469/1053/23. *Єдиний державний реєстр судових рішень*. URL: https://reyestr.court.gov.ua/Review/112481101.