УДК 343.1
DOI https://doi.org/10.32782/2524-0374/2024-10/103

ПРОБЛЕМНІ АСПЕКТИ НЕГЛАСНИХ ЗАХОДІВ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ ПІД ЧАС ВИЯВЛЕННЯ ТА РОЗШУКУ ВІРТУАЛЬНИХ АКТИВІВ, ПОВ'ЯЗАНИХ ІЗ КРИМІНАЛЬНИМИ ПРАВОПОРУШЕННЯМИ

PROBLEM ASPECTS OF COVERT MEASURES OF OPERATIONAL UNITS DURING THE DETECTION AND SEARCH OF VIRTUAL ASSETS RELATED TO CRIMINAL OFFENSES

Ковальський А.В., студент І курсу магістратури
факультету слідчої та детективної діяльності
Національний юридичний університет імені Ярослава Мудрого

Стаття присвячена дослідженню проблемних питань негласних заходів (негласні слідчі розшукові дії, далі – НС(Р)Д; оперативно-розшукові заходи, далі – ОРЗ) оперативних підрозділів під час виявлення та розшуку віртуальних активів, пов'язаних із кримінальними правопорушеннями. Незважаючи на велику кількість праць присвячених дослідженню різних аспектів діяльності оперативних підрозділів у частині проведення негласних заходів, у літературі недостатньо увагу приділено їх особливостям при виявлення та розшуку віртуальних активів.

Метою статті є дослідження та вирішення проблемних питань негласних заходів оперативних підрозділів під час виявлення та розшуку віртуальних активів, пов'язаних із кримінальними правопорушеннями, та обґрунтування значення цих особливостей для практики оперативних підрозділів, органів досудового розслідування у цілому.

Визначено, що найбільш поширеними та суспільно небезпечними кримінальними правопорушеннями, які пов'язані із віртуальними активами є шахрайство з використанням віртуальних активів, легалізація (відмивання) доходів, одержаних злочинних шляхом за допомогою віртуальних активів, надання неправомірної вигоди, придбання, збут наркотичних засобів, фінансування тероризму, тероризм.

Констатовано, що дані кримінальні правопорушення потребують знання особливостей даного явища та специфіки НСРД та ОРЗ.

Розкрито проблеми при проведенні негласних заходів при виявленні, розшуку віртуальних активів та попередженні вчинення кримінального правопорушення, пов'язаного із ними: недоліки Кримінального процесуального кодексу (далі – КПК), збереження доказів, ідентифікація суб'єктів, часові обмеження.

Обґрунтовано, що знання особливостей проведення негласних заходів під час виявлення, розшуку віртуальних активів, пов'язаних із кримінальним правопорушенням є важливим для оперативних підрозділів та досудового розслідування. У більшості практичних ситуаціях наявні підготовчі дії та приховування віртуальних активів, що потребує відповідних технічних знань і навичок для досягнення злочинного результату, при цьому оперативні підрозділи та органи досудового розслідування повинні швидко реагувати та мати також технічні навички для ефективного та вчасного виявлення віртуальних активів. Наголошується, що досить часто під час розшуку та виявлення віртуальних активів є проблема транскордонності та міжнародної співпраці. Виокремлено проблемні аспекти використання оперативно-розшукових засобів після відкриття кримінального провадження. Надзвичайно важливим для досудового розслідування та оперативних підрозділів є знання про суб'єкта та його технічне обладнання під час проведення негласних заходів. Визначено, що, оскільки інформаційні технології та кіберзлочинність постійно вдосконалюються існує необхідність регулювання кращого регулювання засобів оперативно-розшукової діяльності та їх використання, розширення підстав проведення ОРЗ зокрема, задля розкриття вчинених кримінальних правопорушень.

Ключові слова: негласні заходи, оперативні підрозділи, віртуальні активи, досудове розслідування.

The article is devoted to the study of the problematic issues of covert measures (covert investigative investigative actions, hereinafter – NS(R)D; operational and investigative measures, hereinafter – ORZ) of operative units during the detection and search of virtual assets related to criminal offenses. Despite the large number of works dedicated to the study of various aspects of the activity of operational units in the part of conducting covert activities, insufficient attention is paid in the literature to their features in the detection and search of virtual assets.

The purpose of the article is to research and solve problematic issues of covert measures of operational units during the detection and search of virtual assets related to criminal offenses, and to substantiate the significance of these features for the practice of operational units, pretrial investigation bodies as a whole.

It was determined that the most widespread and socially dangerous criminal offenses related to virtual assets are fraud using virtual assets, legalization (laundering) of criminally obtained income with the help of virtual assets, provision of illegal benefits, acquisition, sale of narcotic drugs, financing terrorism, terrorism.

It was established that these criminal offenses require knowledge of the specifics of this phenomenon and the specifics of NSRD and ORZ.

The problems in the implementation of covert measures for the detection and search of virtual assets and the prevention of the commission of a criminal offense related to them are revealed: shortcomings of the Criminal Procedure Code (hereinafter – the Code of Criminal Procedure), preservation of evidence, identification of subjects, time limits.

It is substantiated that knowledge of the specifics of conducting covert measures during the detection and search of virtual assets related to a criminal offense is important for operative units and pre-trial investigation. In most practical situations, there are preparatory actions and concealment of virtual assets, which requires appropriate technical knowledge and skills to achieve a criminal result, while operational units and pre-trial investigation bodies must be quick to respond and also have technical skills for effective and timely detection of virtual assets. It is emphasized that quite often during the search and detection of virtual assets there is a problem of cross-border and international cooperation. Problematic aspects of the use of investigative tools after the opening of criminal proceedings are singled out. Knowledge of the subject and his technical equipment during undercover operations is extremely important for pretrial investigation and operational units. It was determined that, since information technologies and cybercrime are constantly improving, there is a need to better regulate the means of operational and investigative activity and their use, to expand the grounds for conducting an investigation, in particular, to reveal committed criminal offenses.

Key words: covert measures, operative units, virtual assets, pretrial investigation.

Постановка проблеми. Сучасний розвиток інформаційних технологій докорінно змінює суспільство. Разом з тим, з'являються і нові можливості для вчинення кримінальних правопорушень. Кіберзлочинність є нагальною проблемою, з якою веде боротьбу правоохоронна система нашої держави. Одним із найбільш поширених її проявом є використання віртуальних активів як засобу чи способу при вчиненні кримінального правопорушення. Особливої актуальності дане явище набуває в умовах воєнного стану. Зважаючи на це, критично важливим є розробка відповідних сучасних методик негласних заходів та їх вивчення. Ефективність розслідування багато в чому залежить від

правильного розуміння даного явища оперативними підрозділами та їх технічних знань, оскільки саме вони виступають основою під час проведення НС(Р)Д та ОРЗ, побудови та перевірки слідчих версій, збирання доказів для досудового розслідування, що впливає на ефективність кримінального провадження. Більше того, проблематика віртуальних активів у науці кримінального процесу та оперативно-розшукової діяльності залишається дискусійним явищем і потребує подальшого доктринального дослідження.

Аналіз останніх досліджень. Зважаючи на актуальність розслідування кримінальних правопорушень, пов'язаних із віртуальними активами, окремі аспекти дослідження були висвітлені у наступних вітчизняних працях: Я. Т. Яцика, В. А. Шкелебея, О. В. Бондаренка, О. В. Яроцького, О. А. Самойленка, Д. В. Казначеєвої, О. М. Карапетян, В. В. Білинський та інших. Особливої уваги заслуговує робота О. М. Карапетян у співаторстві із В. В. Білинським, у якій була проаналізована проблематика розслідування кримінальних правопорушень пов'язаних із віртуальними активами і було закцентовано увагу на аспектах виявлення та вилучення криптовалюти [1]. Окремо також варто виділити роботу Яцика Т. П. у співавторстві із Шелебеєм В. А., у якій науковці сконцентрувалися на проблемах виявлення криптовалюти через її анонімність, а також технічні особливості щодо приховування слідів вчинення кримінального правопорушення [2]. Прикладом зарубіжного наукового аналізу є робота A. Trozze, де розглядаються превентивні заходи щодо неправомірного заволодіння віртуальними активами на основі смарт-контрактів [3]. Проблематика негласних заходів під час виявлення та розшуку віртуальних активів під час розслідування кримінальних правопорушень у фінансовій сфері була частково висвітлена також у праці S. Saha [4].

Проте питання негласних заходів оперативних підрозділів під час виявлення та розшуку віртуальних активів є недостатньо дослідженим.

Виклад основного матеріалу. Відповідно до статистики звітів міжнародної неурядової організації Chainanalysis, у 2022 році вартість віртуальних активів, які були залучені до кримінальних правопорушень становила 39,6 мільярдів доларів. Тоді як, у 2023 році спостерігалося значне зниження вартості віртуальних активів, які були пов'язані із кримінальними правопорушеннями, до загальної суми 24,2 мільярда доларів. При цьому, ці цифри є нижчими, ніж реальні. Наприкінці 2024 року дані показники скоріше за все зростуть, оскільки виявиться більше незаконних адрес криптогаманців, які були залучені. Значна частина цього зростання відбудеться завдяки ідентифікації раніше невідомих дуже активних адрес криптогаманців [5].

Віртуальні активи є широким поняттям. Воно дозволяє охопити більшість нових інформаційних явищ, таких як усі види криптовалюти, NFT (невзаємозамінні токени), речі в комп'ютерних іграх та інше.

Узагальнено можна виділити такі ознаки віртуальних активів як: цифровий вираз вартості, вільне обертання на ринку віртуальних активів (ринком виступають криптовалютні біржі, різноманітні маркет-плейси, де кожна особа може придбати віртуальний актив), а також наявність чіткої системи ідентифікації за допомогою блокчейн технології. Саме завдяки їй транзакції проводять безпосередньо між учасниками відносин у сфері віртуальних активів. Всі учасники під'єднані до однієї комп'ютерної мережі, яка побудована на блокчейні. Досить часто, транзакції забезпечуються смарт-контрактами, хоча існують поодинокі біржі, які їх не використовують. При цьому забезпечується майже повна анонімність.

Відповідно до Закону України «Про віртуальні активи» (який досі не набрав чинності), віртуальний актив це нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі. Існування та оборотоздатність віртуального активу забезпечується системою забезпечення обороту віртуальних активів [6]. Інше визначення міститься у Законі України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», а саме віртуальний актив – цифрове вираження вартості, яким можна торгувати у цифровому форматі або переказувати і яке може використовуватися для платіжних або інвестиційних цілей [7].

Віртуальні активи можуть стосуватися майже кожного кримінального правопорушення. Втім, найбільш суспільно небезпечні кримінальні правопорушення пов'язані із віртуальними активи відносяться до підслідності Служби безпеки України (далі – СБУ), Національного антикорупційного бюро України (далі – НАБУ). Зокрема, оперативні підрозділи СБУ у Харкові затримали шістьох колишніх посадовців проєктних інститутів України, яких підозрюють у роботі на «Росатом», що перебуває під санкціями. За даними слідства, вони допомагали під'єднати Запорізьку АЕС до «Росатома». Слідство встановило, що підозрювані розробляли науково-дослідну та проєктну документацію для модернізації російських атомних станцій. Фінансування отримували за рахунок криптовалюти. Дії інженерів були викриті на етапі підготовки проєктної документації, що є особливо важливим у ситуаціях, пов'язаних із віртуальними активами. Тим самим українська спецслужба зірвала спроби «Росатома» отримати доступ до стратегічно важливих українських технологій та попередила можливий майбутній терористичний акт [8]. Іншим прикладом може слугувати затримання працівниками НАБУ екс-голови Держспецзв'язку. Зокрема, під час обшуку працівники НАБУ знайшли криптогаманець з 1,5 мільйонів доларів на рахунку. За словами представника Спеціалізованої антикорупційної прокуратури фігурант також мав у своєму розпорядженні 1 201 285 одиниць криптовалюти Tether USDT, що еквівалентно 1 201 928 доларам, і 6,9 біткоїна (265 тисяч доларів), які стосуються кримінального правопорушення [9]. Отже, наразі оперативні підрозділи та органи досудового розслідування досить часто стикаються на практиці із віртуальними активами та різноманітними їх видами. Також віртуальні активи достатньо поширені під час придбання, збуту, наркотичних засобів, шахрайства та у інших кримінальних правопорушень.

Незважаючи на яскраві приклади діяльності оперативних підрозділів, існують проблеми використання оперативно-розшукових засобів під час виявлення та розшуку віртуальних активів. Одним із основних завдань оперативно-розшукової діяльності є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, яке виконується із застосуванням оперативних та оперативно-технічних засобів [10]. Згідно з вимогами ст. 6 Закону України «Про оперативно-розшукову діяльність» підставами для проведення оперативно-розшукової діяльності є наявність достатньої інформації, одержаної в установленому законом порядку, що потребує перевірки за допомогою оперативно-розшукових заходів і засобів, перелік таких підстав є вичерпним. Однак даною статтею не передбачена підстава проведення ОРЗ для розкриття злочинів, а саме встановлення осіб, які вчинили кримінальні правопорушення, зокрема розшуку грошей, цінностей та іншого майна одержаного внаслідок вчинення кримінальних правопорушень. Особливо це актуально при наявності віртуальних активів, оскільки наявні певні проблеми через сутність даного явища і проведенні негласних заходів.

Більше того, у КПК відсутній механізм використання засобів оперативно-розшукової діяльності в ході досу-

дового розслідування під час розкриття кримінальних правопорушень. Відповідно, залучення інших способів, які не передбачені КПК, для отримання доказів тягне за собою їх недопустимість. Проте, відповідно до ст. 40 КПК існує механізм надання доручення слідчого оперативним підрозділам для проведення НС(Р)Д, перелік яких чітко визначений даним Кодексом [11]. При цьому, не передбачена можливість використання таких оперативно-розшукових засобів як програми та інших, які полегшують оперативним підрозділами виявлення та розшук віртуальних активів. Дана прогалина, на нашу думку, не дозволяє оперативним підрозділами та органам досудового розслідування виявляти віртуальні активи ефективно у провадженнях, у яких не встановлено особу. У зв'язку з цим при розслідуванні даних кримінальних правопорушень виникають проблеми з огляду на наступне.

Розшуку та виявленню віртуальних активів, на нашу думку, притаманні наступні особливості:

1. Технологічна складність. Традиційні негласні заходи, передбачені КПК (зокрема зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача; зняття інформації з електронних комунікаційних мереж) потребують великих зусиль та швидкого реагування, часто можуть бути неефективні через використання особами шифрування та анонімних мереж (наприклад TOR).

2. Юридичні обмеження. Чинне законодавство не завжди встигає за розвитком технологій, що створює правові прогалини у застосуванні оперативно-розшукових засобів щодо віртуальних активів.

3. Міжнародний аспект. Транскордонний характер операцій з віртуальними активами ускладнює їх розшук та виявлення, вимагаючи міжнародної співпраці.

4. Ідентифікація суб'єктів. Анонімність користувачів віртуальних активів ускладнює встановлення реальних осіб, причетних до кримінальних правопорушень.

5. Динамічність середовища. Швидка зміна технологій та методів злочинної діяльності вимагає постійного оновлення тактик проведення негласних заходів.

При проведенні НС(Р)Д оперативні підрозділи за дорученням слідчого також можуть стикнутися із схожими проблемами. Зокрема, як було зазначено вище, традиційні негласні заходи, передбачені КПК можуть бути неефективними. Наприклад, під час проведення негласного заходу передбаченого ст. 264 даного Кодексу окрім відповідного унікального шифрованого зв'язку і програмного забезпечення для прикриття кримінального правопорушення, оперативні підрозділи можуть стикнутися з проблемою децентралізованої природи багатьох систем віртуальних активів, що може ускладнити визначення конкретного власника чи утримувача інформації через технологію блокчейн. Більше того, шифрування холодних гаманців, на яких містяться дані про віртуальні активи та самі віртуальні активи ускладнює доступ до інформації через seed – випадкові унікальні фрази, без яких неможливо отримати доступ навіть за допомогою програмного забезпечення. Іншим прикладом може слугувати ситуація, коли особа відома, проте користується анонімними криптообмінниками. При встановленні негласного спостереження в публічних місцях (ст. 269 КПК) особа може скористатися послугами криптообмінника, здійснити обмін віртуальних активів на звичайну валюту. Згодом, дані обмінники використовують так звані міксери (спеціальні методи задля прикриття справжнього походження віртуальних активі). В подальшому відстеження криптовалюти може стати неможливим. Це є досить поширеною практикою. Наприклад, СБУ заблокувала мережу підпільних криптообмінників у столиці. Через нелегальні установи щомісяця проводили до 30 мільйонів гривень, частина з яких йшла на фінансування провокацій до Дня Незалежності України. За інформацією СБУ, підпільні криптообмінники користувалися попитом, оскільки дозволяли проводити анонімні платежі та системно виводити тіньові кошти і переводити в готівку. Послугами цих онлайн-обмінників здебільшого користувалися фізичні особи. Зокрема люди, які отримували кошти із заборонених в Україні електронних гаманців країни-агресора, наприклад, «Яндекс.Деньги», «Qiwi», «Webmoney» тощо [12]. Під час зняття інформації з електронних комунікаційних мереж (ст. 263 КПК) виникає проблема міжнародного характеру операцій з віртуальними активами, що може вимагати співпраці з правоохоронними органами інших країн. Це може бути тривалий процес, тому особа може здійснитися переказ на інші гаманці криптоактиви, скористатися міксером, що позбавить органи досудового розслідування інформації про знаходження віртуальних активів. Відповідно, часові обмеження можуть перешкодити оперативним підрозділам діяти ефективно. Підсумовуючи, існують наступні проблеми проведення негласних заходів: швидкість технологічних змін у сфері віртуальних активів може випереджати законодавчі та процесуальні можливості правоохоронних органів, оперативних підрозділів; необхідність спеціальних знань та технічного забезпечення для ефективного проведення негласних заходів у цій сфері.

Прикладом вітчизняного професійного розвитку може слугувати НАБУ. Зокрема, Національне агентство боротьби із злочинністю Великої Британії (The National Crime Agency) допомагає НАБУ впроваджувати нові інструменти для відстеження коштів, віртуальних активів, отриманих у вигляді хабарів чи вкрадених у держави, та викриття посадовців, причетних до корупційних правопорушень. Така співпраця здійснюється відповідно до Меморандуму про співробітництво у сфері обміну інформацією для боротьби з організованою злочинністю [13]. Важливим також є впровадження системи Maltego Національною поліцією України. Ця система дозволяє масово аналізувати соціальні мережі, веб-сайти, форуми, фінансові операції (у тому числі з віртуальними активами) та інші дії користувачів у мережі інтернет, що може значно допомогти негласним заходам [14].

Висновки. З огляду на вищевикладене, можна зробити наступні висновки. Проблема виявлення та розшуку віртуальних активів, пов'язаних із кримінальними правопорушеннями, є актуальною та складною для оперативних підрозділів та органів досудового розслідування. Існуючі негласні заходи, передбачені чинним законодавством, не завжди ефективні для роботи з віртуальними активами через їх технологічну специфіку. Важливим є підвищення технічної компетентності працівників оперативних підрозділів та слідчих для ефективного проведення негласних заходів у сфері віртуальних активів. Існує необхідність вдосконалення законодавчої бази для покращення роботи оперативних підрозділів під час виявлення та розшуку віртуальних активів, а саме щодо засобів оперативно-розшукової діяльності та їх використання, розширення підстав проведення ОРЗ зокрема, для розкриття вчинених кримінальних правопорушень.

ЛІТЕРАТУРА

1. Карапетян О., Білинський В. Злочинні технології збагачення з використанням криптовалют та особливості їх розслідування. *Актуальні проблеми правознавства*. 2018. № 2. С. 115–118. URL: https://appj.wunu.edu.ua/index.php/appj/article/view/293(дата звернення: 18.10.2024).

2. Yatsyk T. P., Shkelebei V. A. Investigation of criminal offenses related to traffic of virtual assets. *Uzhhorod National University Herald. Series: Law*. 2024. T. 2, № 80. C. 219–223. URL: https://doi.org/10.24144/2307-3322.2023.80.2.34(дата звернення: 18.10.2024).

3. Cryptocurrencies and future financial crime / A. Trozze et al. *Crime science*. 2022. Vol. 11, no. 1. URL: https://doi.org/10.1186/s40163-021-00163-8(дата звернення: 18.10.2024).

4. Cryptocurrency and financial crimes: a bibliometric analysis and future research agenda / S. Saha et al. *Multidisciplinary reviews*. 2024. Vol. 7, no. 8. P. 2024168. URL: https://doi.org/10.31893/multirev.2024168(дата звернення: 18.10.2024).

5. 2024 Crypto Crime Trends from Chainalysis. *Chainalysis*. URL: https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ (дата звернення: 18.10.2024).

6. Про віртуальні активи : Закон України від 17.02.2022 № 2074-IX : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text(дата звернення: 18.10.2024).

7. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 06.12.2019 № 361-IX : станом на 23 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text(дата звернення: 18.10.2024).

8. СБУ: У Харкові інженери за криптовалюту допомагали РФ під'єднати Запорізьку АЕС до "Росатома" | Межа. Новини України. *Межа. Новини України*.URL: https://mezha.net/ua/bukvy/sbu-u-kharkovi-inzhenery-za-kryptovaliutu-dopomahaly-rf-pid-iednaty-zaporizku-aes-do-rosatoma/(дата звернення: 18.10.2024).

9. Економічна правда. Суд арештував 1,5 мільйона доларів криптоактивів ексголови Держспецзв'язку. *Економічна правда*. URL: https://www.epravda.com.ua/news/2023/11/30/707204/(дата звернення: 18.10.2024).

10. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII : станом на 9 серп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text(дата звернення: 18.10.2024).

11. Кримінальний процесуальний кодекс України : Кодекс України від 13.04.2012 № 4651-VI : станом на 7 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text(дата звернення: 18.10.2024).

12. СБУ заблокувала підпільні криптообмінники у Києві. *Фінансовий клуб*. URL: https://finclub.net/news/sbu-zablokuvala-pidpilni-kryptoobminnyky-u-kyievi.html(дата звернення: 18.10.2024).

13. За підтримки британського NCA НАБУ підвищує ефективність розслідування злочинів, вчинених з використанням криптовалют НАБУ офіційний вебсайт. *НАБУ*. URL: https://nabu.gov.ua/news/novyny-za-pidtrymky-brytanskogo-nca-nabu-pidvyshchuye-efektyvnist-rozsliduvannya-zlochyniv-vchynenyh/(дата звернення: 18.10.2024).

14. Case Study: Ukrainian Cyber Police Fights Crime with Maltego. URL: https://www.maltego.com/blog/case-study-ukrainian-cyber-police-fights-crime-with-maltego/(дата звернення: 18.10.2024).