УДК 343.985.7:343.132:343.359.2
DOI https://doi.org/10.24144/2788-6018.2025.05.3.47

ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОКРЕМИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З ВИКОРИСТАННЯМ КРИПТОВАЛЮТИ

Юсупова К.О.,
доктор філософії з права,
старший викладач кафедри кримінальної юстиції
навчально-наукового інституту права та психології
Національної академії внутрішніх справ
ORCID: 0000-0002-8508-3516

Юсупов В.В.,
доктор юридичних наук, професор,
провідний науковий співробітник
науково-дослідної лабораторії
з проблем криміналістичного забезпечення та судової експертології
Національної академії внутрішніх справ
ORCID: 0000-0001-5216-4144

Марчук Р.П.,
кандидат юридичних наук, доцент,
директор Академії фінансового моніторингу
ORCID: 0009-0005-2108-4375

Юсупова К.О., Юсупов В.В., Марчук Р.П. Особливості проведення окремих слідчих (розшукових) дій під час розслідування кримінальних правопорушень, пов'язаних з використанням криптовалюти.

Досліджено проведення огляду, обшуку, допиту, залучення експерта у кримінальних провадженнях про незаконні дії з криптовалютою. Зазначено про необхідність володіння слідчим знаннями про сутність та механізм обігу різних видів віртуальних активів, що є однією з умов успішного досудового розслідування. Наголошено на необхідності залучати спеціаліста під час розслідування кримінальних правопорушень, пов'язаних з використанням криптоактивів. До таких спеціалістів віднесено: фахівців у сфері інформаційних технологій, осіб, які пройшли навчання у сфері криптовалюти та блокчейну, вузькопрофільних працівників Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, Державного фінансового моніторингу, працівників Департаменту кіберполіції Національної поліції та деяких інших. Головною метою огляду у кримінальних провадженнях про незаконні дії з криптовалютою є виявлення, аналіз і фіксація комп'ютерних даних на різних електронних пристроях, що відображають виконані транзакції з віртуальними активами. Особливостями обшуку під час розслідування кримінальних правопорушень, пов'язаних з використанням криптовалюти, є наявність належних процесуальних підстав для проведення слідчої (розшукової) дії, зокрема рішення Вищого антикорупційного суду у визначених випадках, фіксація процесу всієї дії фото і відеозйомкою, технічні заходи щодо доступу до криптогаманця обшукуваної особи, забезпечення таємниці фіксації і зберігання паролів доступу до електронних гаманців з наявними коштами – предметом кримінального правопорушення. Типовою слідчою (розшуковою) дією є допит потерпілого і підозрюваного. Встановлено, що допит спрямований на деталізацію і уточнення даних про вид криптовалюти, проведені транзакції з нею, особливості збереження паролів, кодів, seed-фраз доступу до криптогаманця. З'ясовано, що поширеною судовою експертизою у кримінальних провадженнях про незаконні дії є комп'ютерно-технічна. За необхідності її поєднання із спеціальними економічними і технічними знаннями, може призначатися комплексна експертиза цифрових активів, заснованих на технології блокчейн. Розглянуто особливості складання протоколів слідчих (розшукових) дій і додатків до них, довідок спеціалістів.

Ключові слова: кримінальне провадження, слідчі (розшукові) дії, спеціальні знання, віртуальні активи, критповалюта, огляд, обшук, допит, залучення експерта, протокол слідчої (розшукової) дії.

Yusupova K.O., Yusupov V.V., Marchuk R.P. Features of conducting certain investigative (search) actions during the investigation of criminal offenses related to the use of cryptocurrency.

The examination, search, interrogation, and involvement of an expert in criminal proceedings on illegal actions with cryptocurrency are studied. The necessity of the investigator to have knowledge of the essence and mechanism of circulation of various types of virtual assets is noted, which is one of the conditions for a successful pre-trial investigation. The necessity of involving a specialist in the investigation of criminal offenses related to the use of crypto-assets is emphasized. Such specialists include: specialists in the field of information technology, persons who have been trained in the field of cryptocurrency and blockchain, narrow-profile employees of the National Agency of Ukraine for the Identification, Search, and Management of Assets Obtained from Corruption and Other Crimes, the State Financial Monitoring, employees of the Cyber Police Department of the National Police, and some others. The main purpose of the inspection in criminal proceedings on illegal actions with cryptocurrency is to identify, analyze and record computer data on various electronic devices that reflect the transactions performed with virtual assets. The features of the search during the investigation of criminal offenses related to the use of cryptocurrency are the presence of appropriate procedural grounds for conducting an investigative (search) action, in particular, the decision of the Supreme Anti-Corruption Court in certain cases, recording the process of the entire action by photo and video recording, technical measures for access to the crypto wallet of the person being searched, ensuring the secrecy of recording and storing access passwords to electronic wallets with available funds - the subject of a criminal offense. A typical investigative (search) action is the interrogation of the victim and the suspect. It has been established that the interrogation is aimed at detailing and clarifying data on the type of cryptocurrency, transactions performed with it, features of storing passwords, codes, seed phrases for accessing the crypto wallet. It was found that a common forensic examination in criminal proceedings on illegal actions is computer-technical. If necessary, its combination with special economic and technical knowledge can be assigned a comprehensive examination of digital assets based on blockchain technology. The features of drawing up protocols of investigative (search) actions and annexes to them, and expert certificates are considered.

Key words: criminal proceedings, investigative (search) actions, special knowledge, virtual assets, cryptocurrency, inspection, search, interrogation, involvement of an expert, protocol of investigative (search) actions.

Постановка проблеми. Нині криптовалюта є фінансовим засобом та платіжним інструментом, водночас – й предметом злочинних посягань. Правопорушники стали більш досвідченими у використанні криптовалюти з протиправною метою. Незаконне використання віртуальних активів переважно пов’язане з «відмиванням» грошей, шахрайством, онлайн торгівлею, оплатою різних видів злочинної діяльності. Розслідування кримінальних правопорушень, пов’язаних з використанням криптовалюти, ускладнено їх особливостями: латентністю; спроможністю швидкого знищення або зміни цифрових слідів; виникненням проблеми під час огляду децентралізованих комп’ютерних систем, документування та експертизи слідів пам’яті технічних пристроїв, в онлайн мережі чи на фізичних носіях інформації; короткочасністю зберігання інформації, здатної виступити як доказ [1, с. 180]. Слідчий, розслідуючи кримінальні правопорушення, пов’язані з використанням криптовалюти, повинен володіти знаннями про сутність та механізм обігу різних видів віртуальних активів, а також майстерно використовувати основний процесуальний інструментарій – слідчі (розшукові) дії (СРД).

Стан опрацювання проблематики. Вітчизняні вчені досліджували різну тематику, пов’язану з обігом віртуальних активів, вчиненням кримінальних правопорушень з криптоактивами та протидією правоохоронними органами відповідній незаконній діяльності. В аспекті загальних питань розслідування кримінальних правопорушень, пов’язаних з використанням криптовалюти, досліджувалися властивості різних віртуальних активів (Л.В. Товкун, В.В. Черниш, І.В. Юдіна), організаційні принципи роботи з ними (В.О. Ковтун, О.В. Манжай, В.В. Носов, Є.В. Панченко), розслідування «відмивання» грошей через криптовалютні транзакції (О.О. Загуменний, М.В. Попович), розслідування злочинів, пов’язаних з фінансуванням криптовалют, тероризмом та збройною агресією (В.В. Козій, А.В. Мовчан, І.А. Федчак, О.А. Шляховський). У напрямі кримінальної процесуальної діяльності із розслідування незаконних дій з віртуальними активами українські дослідники аналізували проблеми доказування у кримінальних провадженнях про злочини щодо незаконного заволодіння криптовалютою (В.В. Козій), захисну діяльність у цих кримінальних провадженнях (Р.А. Лукінчук, А.В. Пенкіна), негласні СРД (О.А. Самойленко, К.В. Тітуніна) та ін. Водночас, узагальнення типових, найбільш поширених СРД у кримінальних провадженнях про незаконні дії з криптовалютою, висвітлення процесуальних особливостей їх проведення, нині є малодослідженими.

Метою статті є дослідження особливостей окремих типових СРД під час розслідування кримінальних правопорушень, пов'язаних з використанням криптовалюти, узагальнення криміналістичних рекомендацій щодо удосконалення їх проведення.

Викладення основного матеріалу. Для виявлення та відслідковування незаконної діяльності у мережах технології «блокчейн» використовуються спеціальні знання та відповідно спеціальне програмне забезпечення [2]. У зв'язку з цим під час розслідування кримінальних правопорушень, пов'язаних з використанням криптовалюти, рекомендується використовувати допомогу спеціалістів. Процесуальні дії, які планується проводити, мають бути попередньо сплановані, слідчому не зайвим буде проконсультуватися з відповідними спеціалістами, вирішити питання про їх залучення до СРД, «прорахувати» можливі слідчі ситуації у зв'язку з контактуванням із особою, щодо якої здійснюватиметься захід.

Очевидно, що спеціалістами у цій категорії справ можуть бути фахівці у сфері інформаційних технологій (ІТ), а також інші особи, які, наприклад, мають сертифікати чи свідоцтва про проходження тренінгів або навчальних курсів у сфері криптовалюти та блокчейну. Консультації із спеціалістом слід здійснювати ще на етапі планування та підготовки до проведення вилучення криптовалюти, а не безпосередньо під час її вилучення [3, с. 481]. Також до СРД можна залучати фахівців Національного агентства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів (АРМА). На сайті АРМА міститься типовий зразок відповідного звернення представників правоохоронних органів [4]. Іншими фахівцями є працівники Держфінмоніторингу. Необхідну допомогу нададуть й поліцейські Департаменту кіберполіції Національної поліції України – технічні фахівці.

Використання спеціальних знань і навичок спеціаліста фіксується у протоколі СРД, додатках до нього. Можлива й підготовка довідок спеціаліста у сфері криптовалюти як окремого процесуального документа. У такій довідці особа, маючи відповідні спеціальні знання, може зазначити всі транзакції з криптовалютою в електронному гаманці підозрюваного, описати особливості виду криптовалюти, вказати спеціальне програмне забезпечення, яке було застосовано спеціалістом та ін. Ця довідка буде вважатися документом, яка відповідно до ст. 99 КПК України, є джерелом доказів.

Як зазначають О.А. Самойленко і К.В. Тітуніна, матеріали, отримані в результаті використання спеціального програмного забезпечення, можуть залучатися до процесу доказування, по-перше, як матеріали, що супроводжують (або доповнюють) показання осіб, по-друге, як документи, що не мають самостійного процесуального значення, але були отримані як довідки спеціалістів – додатки до протоколів СРД [5, с. 418].

Типовою першочерговою СРД у кримінальних провадженнях, пов'язаних з використанням криптовалюти, є огляд. Відповідно до ч. 1 ст. 237 КПК України з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей, документів та *комп'ютерних даних*. Під час огляду у цій категорії кримінальних проваджень слідчий, прокурор залучають спеціалістів. Огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у протоколі інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі) [6]. Відповідні дані можуть відображатися й в додатках до протоколу або довідках спеціалістів. Якщо під час огляду (обшуку) слідчий виявляє апаратний криптовалютний гаманець, то мають бути вжиті заходи до знаходження паролю для доступу до нього. Те саме стосується і смартфонів, планшетів та ноутбуків чи смарт-годинників підозрюваного.

Іншою типовою СРД під час розслідування незаконних дій з криптовалютою є *обшук*. Загальний порядок обшуку передбачений в статтях КПК – ст. 234, 235, 236 та ін. [6]. Обшук проводиться на підставі ухвали слідчого судді місцевого загального суду, в межах територіальної юрисдикції якого знаходиться орган досудового розслідування, а у кримінальних провадженнях щодо злочинів, віднесених до підсудності Вищого антикорупційного суду (ВАКС), – на підставі ухвали слідчого судді ВАКС. У справах про незаконні дії з криптоактивами отримання ухвал від ВАКС є частими явищем. Наприклад, це такі провадження (справи ВАКС): № 991/3721/22; № 991/2399/23; № 991/1512/23; № 991/10335/23 [7].

При проведенні обшуку може бути присутній потерпілий, підозрюваний, захисник, представник та інші учасники кримінального провадження. Слідчий для участі в обшуку залучає відповідних спеціалістів. Особи, які володіють інформацією про зміст комп'ютерних даних та особливості функціонування комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, можуть повідомити про це слідчого, прокурора під час здійснення обшуку, відомості про що вносяться до протоколу обшуку. Обшук житла чи іншого володіння особи в обов'язковому порядку фіксується за допомогою відеозапису.

Пропонуємо алгоритм пошуку та особливості вилучення криптовалюти під час обшуку: пошук гаджетів (комп'ютерів, ноутбуків, планшетів, смартфонів, тощо), де знаходиться програмне забезпечення, за допомогою якого можна отримати доступ до криптовалюти; пошук паролів для доступу до акаунтів на криптовалютних біржах чи до програмного забезпечення для доступу до криптовалюти; пошук мнемонічних фраз (seed-фраз), за допомогою яких можна відновити доступ до електронних гаманців, на яких зберігається криптовалюта; пошук публічних та приватних ключів доступу до криптовалюти; за потреби і в разі технічної можливості подолання системи логічного захисту, яка встановлена на гаджетах підозрюваних осіб з метою одержання доступу до криптовалюти; безпосередній доступ до криптовалюти, тобто введення логінів, паролів, мнемонічних фраз та іншої необхідної інформації, що надає можливість контролювати електронні гаманці з криптовалютою чи облікові записи на криптовалютних біржах [3, с. 483]; фіксація існуючого стану рахунку і виконаних транзакцій; вилучення виявленої криптовалюти, тобто її перерахування на контрольований правоохоронним органом електронний гаманець; вжиття заходів до таємного збереження приватних ключів, паролів та мнемонічних фраз від криптовалюти, що унеможливлює доступ до неї будь-яких сторонніх осіб; відображення у протоколі СРД, додатках до нього, довідці спеціаліста відомостей про хід та результати.

У протоколах огляду, обшуку мають бути чітко зазначені наступні дані: який вилучений гаджет оглядається, які його повні ідентифікаційні дані (IMEI, номери сім-карт, яке програмне забезпечення для зберігання криптовалюти на ньому встановлено, чи обмежено доступ до нього системою логічного захисту, яким чином її подолали, назва криптовалюти, її кількість, яким способом отримано доступ до криптовалюти, тобто які логін та пароль чи мнемонічні фрази введено, повні дані електронних гаманців, на яких знаходиться криптовалюта, її баланс та дані всіх транзакцій, тобто публічні ключі (публічні адреси) криптовалюти, хеші транзакцій та час їх проведення, а також її баланс. У протоколі не вказуються приватні ключі, мнемонічні фрази та паролі, за допомогою яким можливо отримати доступ до криптовалюти [3, с. 483].

При вилученні смартфона, у якому виявлено дані про електронний криптогаманець, криптододатки, скріншоти або фотографії seed-фраз тощо, слід все детально описати в протоколі. Адже такі відомості є вагомими доказами роботи особи з криптовалютою. Наприклад, відповідно до ухвали слідчого судді ВАКС від 4 жовтня 2022 року у справі № 991/3721/22, факт володіння криптовалютою підтверджувався наявністю на телефоні підозрюваного фотографій seed-фраз та листування щодо операцій, які збігалися з активністю у публічних адресах. На криптовалюту підозрюваного було накладено арешт: криптовалюта Tether (USDT) у кількості 25377,8 одиниць (що станом на 28.07.2022 становить 25383,82 доларів США), Tron (TRX) у кількості 116,770185 одиниць (що станом на 28.07.2022 становить 8 доларів США); криптовалюта Tether (USDT) у кількості 32003 одиниць (що станом на 28.07.2022 становить 32010,52 доларів США), Ethereum (ETH) у кількості 0,006163 одиниць (що станом на 28.07.2022 становить 10 доларів США) [8]. В іншому рішенні ВАКС також посилався на наявність криптовалютних додатків, історії їх використання та фотографій seed-фраз на мобільному телефоні [9].

Важливе значення під час розслідування незаконних дій з криптоактивами має така СРД як *допит*. Допит – це передбачена кримінальним процесуальним законом слідча (розшукова) або судова дія, яка являє собою процес одержання слідчим (прокурором, судом) відомостей щодо обставин кримінального провадження під час спілкування двох чи більше осіб з метою забезпечення швидкого, повного, неупередженого розслідування, судового розгляду й виконання інших завдань кримінального провадження, які визначені ст. 2 КПК України [10, с. 644]. Загальний порядок проведення допиту та окремі особливості допиту визначені у ст. 224–227, 232 та деяких інших КПК України. У випадках, коли потерпілий від злочину, пов'язаного з використанням криптовалюти, подав заяву до правоохоронного органу, першою СРД є його допит. При допиті потерпілого має бути отримано якомога більше інформації, яка дозволить вибудовувати правильні версії та їх перевіряти. Наприклад, потерпілий має зазначити адресу транзакцій, дані хешування свого криптовалютного гаманця. Слід отримати максимально повні дані про вчинення злочину, які фіксуються у протоколі допиту. Можуть виготовлятися додатки до протоколу допиту.

Після проведення першочергових СРД слідчий невідкладно призначає *судові експертизи* відповідно до тих об'єктів, які є у його розпорядженні. Залучення експерта у кримінальному провадженні регламентовано ст. 69, 242, 243, 244 КПК України. Як зазначає І.В. Юдіна, на сьогоднішній день криптавалюта може бути об'єктом судової економічної експертизи, судової комп'ютерно-технічної експертизи, судової експертизи електронних комунікацій [11, с. 332]. Більшість дослідників робить наголос на комп'ютерно-технічній експертизі при необхідності досліджувати об'єкти, пов'язані з обігом криптовалюти. Саме комп'ютерно-технічна експертиза дає змогу встановити технічні обставини, пов'язані з операціями з криптовалютою, визначити її походження та належність конкретній

особі. Об'єктами експертного дослідження виступатимуть записи на машинних носіях інформації, які відшукуються і технічно інтерпретуються в процесі провадження комп'ютерно-технічної експертизи [13, с. 218].

Залежно від поставлених запитань до експерта, судова експертиза криптовалюти може бути *комплексною*, оскільки потребує сукупності спеціальних знань, які застосовуються для розв'язання різних завдань [11, с. 332]. Зауважимо, що нині відсутня методика судової експертизи з дослідження цифрових активів, заснованих на технології блокчейн.

З урахуванням відносно нового виду грошового обігу – віртуальних активів у виді криптовалюти, відповідної регулюючої правової бази, що формується, при виникненні неоднозначності у процесуальних питаннях щодо дій уповноважених осіб, слід керуватися ч. 6 ст. 9 КПК України, де зазначено про застосовування загальних засад кримінального провадження, а саме тих, які передбачено ч. 1 ст. 7 КПК України (верховенство права, законність, рівність перед законом і судом, повага до людської гідності, тощо) [6]. При цьому уповноважена особа враховує слідчу і судову практику, рішення судів міжнародних інстанцій у справах щодо віртуальних активів.

Висновки. Таким чином, у кримінальних провадженнях про злочини, пов'язані з використанням криптоактивів, типовими СРД є огляд, обшук, допит, залучення експерта. Слідчий використовує загальні положення проведення цих СРД з обов'язковим використанням допомоги відповідного спеціаліста. При можливій невизначеності слідчого щодо конкретних дій з предметами, пов'язаними з криптоактивами учасника СРД, він діє відповідно до загальних засад кримінального провадження, передбачених у ст. 7 КПК України. До розслідування кримінальних правопорушень, пов'язаних з використанням криптовалюти, зокрема проведення СРД, слідчий залучає спеціалістів. Ними можуть бути: фахівці у сфері ІТ, особи, які пройшли навчання у сфері криптовалюти та блокчейну, вузькопрофільні працівники АРМА, Держфінмоніторингу, працівники Департаменту кіберполіції Національної поліції та інші фахівці у комп'ютерних технологіях і програмному забезпеченні. Слідчі (розшукові) дії у кримінальному провадженні про незаконні дії з криптовалютою фіксуються у протоколі, додатках до нього, а також за допомогою засобів фото і відеофіксації. Залучений спеціаліст може складати довідки з описом і деталізацією ознак певних об'єктів і процесів, що стосуються обігу віртуальних активів особи – учасника СРД та застосованого спеціального програмного забезпечення. Особливостями складання відповідних процесуальних документів є вжиття заходів щодо втаємничення приватних ключів, паролів та мнемонічних фраз доступу до криптовалюти і відновлення електронного гаманця підозрюваної особи, на який накладено арешт.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бурбело Б.А. Криміналістичні основи протидії кіберзлочинності. *Актуальні питання розслідування кіберзлочинів:* мат. міжнар. наук.-практ. конф. (Харків, 10 груд. 2013 р.) Харків: ХНУВС, 2013. С. 179–182.
2. Petrova M. Integration of the information processes. Automation and unification of the judicial system. *Економіка розвитку.* 2017. № 2(82). С. 50–59.
3. Козій В. В. Порядок та особливості вилучення у кримінальному провадженні незаконно здобутої криптовалюти. *Юридичний науковий електронний журнал*. № 2/2023. С. 479–483. https://doi.org/10.32782/2524-0374/2023-2/113.
4. Співробітництво з правоохоронними органами, надання роз'яснень, методичної та консультаційної допомоги правоохоронним органам: оф. сайт Агенства з рошуку та менеджменту активів. URL: https://arma.gov.ua/spivrobitnytstvo.
5. Самойленко О. А., Тітуніна К. В. Типові криміналістичні засоби розслідування кримінальних правопорушень, пов'язаних із використанням криптовалют. *Актуальні питання у сучасній науці.* № 7(13). 2023. С. 409–420. https://doi.org/10.52058/2786-6300-2023-7(13)-409-420.
6. Кримінальний процесуальний кодекс України: Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17.
7. Єдиний державний реєстр судових рішень: оф. сайт. URL: https://reyestr.court.gov.ua/
8. Ухвала слідчого судді Вищого антикорупційного суду від 4 жовт. 2022 р. у справі № 991/3721/22. URL: https://reyestr.court.gov.ua/Review/106662256.
9. Вирок Вищого антикорупційного суду від 27 листоп. 2024 р. у справі № 991/1512/23. URL: https://reyestr.court.gov.ua/Review/123349217.
10. Криміналістика: підручник / [В.М. Шевчук, В.А. Журавель, В.Ю. Шепітько та ін.]; за заг. ред. В.М. Шевчука. Харків: Право, 2024. 1008 с.
11. Юдіна І.В. Криптовалюта як спеціальний об'єкт судової експертизи: зб. мат. VII міжнар. молод. наук. юрид. форуму (Київ, 16-17 травня 2024 р.). Київ: НАУ, 2024. С. 331–334.

12. Лукінчук Р., Пенкіна А. Хто володіє криптою? Як це довести у кримінальному процесі. *Юридична газета.* № 4(792). 2024. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/hto-volodie-kriptoyu-yak-ce-dovesti-u-kriminalnomu-procesi.html.
13. Усата Г.О., Горошко В.В. Особливості проведення судових експертиз при розслідуванні злочинів, вчинених з використанням криптовалюти. *Актуальні аспекти криміналістичного та психологічного забезпечення правоохоронної діяльності:* мат. наук.-практ. інтернет-конф. (Одеса, 23 квіт. 2021 р.). Одеса, 2021. С. 214–218.