ISSN 2072–8670 (Print)
НАУКА І ПРАВООХОРОНА
NAUKA I PRAVOOKHORONA
DOI (Issue): https: //doi.org/10.36486/np.2022.4(58)
Issue 4(58) 2022

КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА. СУДОВА ЕКСПЕРТИЗА. ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 343.13

Мовчан Анатолій Васильович,
доктор юридичних наук, професор,
професор кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ
м. Львів, Україна
ORCID ID 0000-0002-6997-6517
Козій Василь Васильович,
кандидат юридичних наук, докторант кафедри
оперативно-розшукової діяльності Львівського державного
університету внутрішніх справ м. Львів, Україна
ORCID ID 0000-0002-8221-6678

ОСНОВИ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ЩОДО НЕЗАКОННОГО ЗАВОЛОДІННЯ КРИПТОВАЛЮТОЮ

Статтю присвячено дослідженню основ розслідування злочинів щодо незаконного заволодіння криптовалютою. Проаналізовано поняття криптовалюти, особливості її обігу і функціонування, визначено проблемні питання розслідування злочинів щодо незаконного заволодіння криптовалютою, які підлягають вирішенню як на науковому рівні, так і у практичній діяльності слідчих органів досудового розслідування та прокурорів. Визначено основні способи вчинення злочинів цієї категорії та сформульовано практичні рекомендації щодо методики і тактики розслідування незаконного заволодіння криптовалютою.

Ключові слова: *криптовалюта, досудове розслідування; злочини у сфері криптовалют; блокчейн; незаконне заволодіння криптовалютою; розслідування незаконного заволодіння криптовалютою.*

Упродовж останніх років таке поняття, як криптовалюта, все більше проникає у життя людей. Бурхливого розвитку набули промисловий та побутовий майнінг (тобто видобування криптовалюти), торгівля криптовалютою на централізованих та децентралізованих (DeFi) онлайн біржах та обмінних ресурсах; багато людей тримають у ній заощадження, сплачують нею за товари та послуги, дарують, передають у спадок тощо.

Проте криптовалютою цікавляться не тільки пересічні громадяни, а й злочинці, а це призводить до того, що власники криптовалюти стикаються з її втратою внаслідок незаконного заволодіння. На жаль, будь-який власник криптовалюти одного ранку може прокинутися і виявити, що вся його криптовалюта зникла із

DOI (Article): https: //doi.org/10.36486/np.2022.4(58).17

криптовалютного гаманця або онлайн-біржа, де вона зберігалася, зламана хакерами і все викрадено, або всі його багатотисячні чи навіть мільйонні у доларах США криптовалютні активи внаслідок участі у скам-проєкті віднині коштують лише кілька центів.

Для власників криптовалюти та практично усіх, хто задіяний у криптоіндустрії, у перших числах листопада 2022 р. стало новиною банкрутство третьої за розміром у світі криптовалютної біржі FTX. Так, FTX розпочала процедуру банкрутства в США, а її виконавчий директор Сем Бенкман-Фрід пішов у відставку після кризи ліквідності у компанії, яка викликала втручання регуляторів по всьому світу. FTX та її афілійований криптовалютний фонд Alameda Research і близько 130 інших компаній розпочали добровільне провадження у справі про банкрутство за статтею 11 у штаті Делавер [1].

Аналітична компанія Nansen, що займається розслідуванням банкрутства однієї з найбільших криптобірж FTX, зауважила таємничий витік приблизно 447 млн доларів. Засновника FTX Сема Бенкмана-Фріда допитала поліція та регулятори Багамських островів [2].

Ще через кілька днів Нік Перкоко, директор з безпеки американської криптовалютної біржі Kraken, оголосив, що їм відоме ім'я "хакера", який вивів, за різними оцінками, до 600 мільйонів доларів із криптовалютної біржі FTX, що збанкрутувала. Як і припускали учасники криптовалютної спільноти, за виведенням коштів стоїть хтось зі співробітників компанії, – у Kraken підтвердили цю інформацію, не назвавши при цьому конкретного імені. При цьому воно їм відомо, оскільки шахрай раніше пройшов процедуру KYC (KYC – процедура верифікації "знай свого клієнта" або скорочено know your customer" – авт.) на платформі, а відповідно залишив персональні дані щодо себе [3].

Проте до цього часу розслідування злочинів, пов'язаних із незаконним заволодінням криптовалютою, є абсолютно новим у роботі правоохоронних органів. Також наразі в Україні немає й відповідних наукових досліджень, які б стосувалися тематики розслідування незаконного заволодіння криптовалютою. Окремі питання, які стосуються протидії кіберзлочинності та побічно сфери обігу криптовалют, містяться у працях В. Іванюк, Д. Казначеєвої, А. Дорош, О. Амеліна, П. Біленчука, Р. Благути, В. Болгова, В. Бутусова, С. Буяджи, А. Войцехівського, Г. Власової, Н. Гадіона, О. Гладуна, С. Демедюка, В. Захарова, О. Іванченка, А. Марущака, А. Мовчана, А. Орлеана, М. Погорецького, К. Тітуніна, М. Швеця, О. Юрченка та інших науковців.

Метою статті є визначення основ розслідування злочинів щодо незаконного заволодіння криптовалютою та знаходження способів їх вирішення.

Для розуміння того, які виклики постають перед органами досудового розслідування і як їх вирішувати у контексті розслідування незаконного заволодіння криптовалютою, необхідно з'ясувати поняття криптовалюти, її види та основи функціонування і обігу. Ці знання є фундаментом, який дозволяє визначати методику і тактику їх розслідування.

Найпершою криптовалютою у світі є біткоїн (BTC), історія якого почалася у 2008 році з того, що особа чи група осіб під псевдонімом Сатоши Накамото опублікувала файл, у якому визначила протокол і принцип роботи унікальної

DOI (Article): https: //doi.org/10.36486/np.2022.4(58).17

електронної системи на основі блокчейну – біткоїна. З технічного погляду біткоїн – це цифровий електронний актив, цифрові грошові кошти, які обертаються у децентралізованій, пірінговій (від англ. "peer-to-peer", "P2P" – рівний рівному обмін файлами в мережі, який базується на рівноправності учасників) електронній платіжній системі, заснованій на публічно доступній книзі обліку під назвою блокчейн ("блокчейн" у перекладі з англійської – "ланцюг блоків").

Проте біткоїн не єдина криптовалюта у світі. Відповідно до онлайн-ресурсу CoinmarketCap, станом на 16 листопада 2022 року існувало 21 778 різних криптовалют, 524 онлайн-біржі, а загальна капіталізація ринку криптовалют становила понад 828 мільярдів доларів США. При цьому домінування біткоїну становило понад 38,5 %, а ефіріуму (ETH) – 17,8 % [4].

Основними способами отримати криптовалюту є її придбання за грошові кошти на спеціалізованих біржах, найвідомішими з яких є Binance, Huobi, Bitfinex, Whitebit тощо або ж отримати її за допомогою майнінгу, який полягає у наданні обчислювальних потужностей комп'ютера або спеціалізованого обладнання (відеокарт, айсік-майнерів, процесорів, пам'яті) для складних обчислень, взятих за основу в системах криптовалют.

Ключовими особливостями більшості криптовалют є децентралізація, адже відсутній єдиний емісійний центр, яким є центральні банки та уряди країн світу у випадку емісії грошових коштів, а також те, що будь-яку транзакцію, тобто відправлення криптовалюти із однієї електронної адреси (електронного гаманця) на іншу (інший електронний гаманець), за деякими винятками, скасувати неможливо. Загалом криптовалюта – це віртуальні електронні активи, які являють собою унікальні криптографічні коди, існування яких ґрунтується на правилах криптографії. Різні країни світу у своєму національному законодавстві по-різному підходять до сприйняття криптовалюти та умов її обігу, від несприйняття та повної заборони до повного визнання платіжним засобом.

Так, у Сальвадорі біткоїн визнано офіційним платіжним засобом. 07 вересня 2021 року в Сальвадорі набрав чинності закон про визнання біткоїна легальним засобом розрахунків. Уряд влаштував безкоштовну роздачу криптовалюти, щоби зробити її привабливішою. Кожен дорослий громадянин Сальвадора, в якій би країні він не знаходився, отримав можливість завантажити на свій смартфон офіційний криптовалютний гаманець Chivo і після реєстрації отримати на нього електронні монети вартістю $30 – приблизно 0,0005 біткоїна [5].

Разом з тим, повна заборона на операції з криптовалютою введена в Алжирі, Марокко, Лівії, Намібії та Зімбабве [6, с. 262].

В Україні упродовж багатьох років ринок криптовалют залишався практично неврегульованим. Лише 17.02.2022 ухвалено Закон України "Про віртуальні активи", який визнає криптовалюту віртуальним активом, і відповідно до п. 1 ст. 1 якого 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. Віртуальний актив може посвідчувати майнові права, зокрема права вимоги на інші об'єкти цивільних прав [7].

DOI (Article): https: //doi.org/10.36486/np.2022.4(58).17

Тактика і методика розслідування злочинів щодо незаконного заволодіння криптовалютою залежить від основних двох чинників: 1) від загальної характеристики та особливостей функціонування блокчейну тієї чи іншої криптовалюти; 2) від способу вчинення того чи іншого кримінального правопорушення.

Передусім визначимо основні види криптовалют та деякі особливості їх функціонування і обігу. Як ми відзначали вище, біткоїн – перша криптовалюта. Альткоїни – всі інші, створені після біткоїна. Деякі з них є форками біткоїна, тобто за основу їх функціонування взято програмний код біткоїна, але із тими чи іншими змінами, наприклад Лайткоїн (Litecoin), який є одноранговою валютою і платіжною мережею. На відміну від Біткоїна криптовалюта Ethereum (ефіріум) – це перший у світі програмований блокчейн, який дозволяє розробникам створювати і розгортати децентралізовані додатки (DApps), а також смарт-контракти. Криптовалюти також поділяються на децентралізовані і стейблкоїни (стабільні монети). Курс децентралізованих криптовалют постійно змінюється, іноді дуже швидко і значно, адже ані держава, ані її регулюючі органи не мають прямого впливу на курс тієї чи іншої криптовалюти. Стейблкоїни – це альткоїни, курс яких забезпечений активами, наприклад фіатними валютами чи товарними цінностями, і курс стейблкоїну відповідає вартості активу, який його забезпечує, наприклад 1 долару США чи 1 євро, вартості одинці виміру золота, нафти тощо. Забезпечені стейблкоїни поділяються на фіатні та товарні. Найвідомішими стейблкоїнами є USDT компанії Tether та USDC консорціуму Centre, до якого входять біржа Coinbase і компанія Circle, яка і є основним розробником стейблкоїну. Ці токени забезпечені доларом США у співвідношенні 1 до 1. При надходженні валюти компанія випускає нові токени, а при виконанні своїх зобов'язань "спалює" їх, тобто зменшує їх кількість на відповідну суму. Але є і незабезпечені стейблкоїни – криптовалютні та алгоритмічні, у яких немає забезпечення як такого. Їх курс регулюється автоматичним смарт-контрактом, який, залежно від ринкової ціни валюти, зменшує або збільшує їх кількість в обігу, яку взято за основу. Проте токени – це не зовсім криптовалюта, а швидше грошовий сурогат або ж одиниця обліку на цифровому балансі. Вони можуть випускатися як централізовано, так і децентралізовано та не завжди базуються на технології блокчейну, зазвичай посвідчують право на щось.

Будь-яка криптовалюта умовно складається із набору символів – букв та цифр, і при цьому із цих самих символів складається адреса гаманця, так званий публічний ключ, який генерується системою, який потрібно знати тому, хто збирається переказати на нього певну суму тієї чи іншої криптовалюти. Наприклад, адреса електронного гаманця біткоїна може мати такий вигляд: 1JNzanNTkCLF4 VrMCt3ByuLu5nje3Zvq1i. Проте є ще приватний ключ, який не можна передавати нікому, так як останній дозволяє у блокчейні біткоїна підтвердити, що відповідна кількість криптовалюти знаходиться на вказаному гаманці, тобто за вказаною адресою у блокчейні. Володіти криптовалютою можна, якщо мати електронний гаманець та приватні ключі. У випадку ж, коли криптовалюта знаходиться на біржі, то і приватні ключі теж знаходяться на біржі, у разі зламу біржі чи викрадення з неї криптовалюти відповідно власник її також втрачає.

DOI (Article): https: //doi.org/10.36486/np.2022.4(58).17

Методика і тактика розслідування злочинів цієї категорії залежить також від видів і способів вчинення конкретних злочинів. Моніторинг відкритих джерел та засобів масової інформації, Єдиного державного реєстру судових рішень та вивчення слідчої і судової практики свідчить про те, що до основних видів незаконного заволодіння криптовалютою можна віднести:

1) злам криптовалютних бірж та електронних гаманців фізичних осіб і виведення криптовалюти на біржі, обмінні ресурси або інші електронні гаманці, у т.ч. з використанням так званих "міксерів", які унеможливлюють відстеження подальшого руху криптовалюти;

2) викрадення криптовалюти самими біржами і подання заяв про злам біржі хакерами та виведення криптовалюти на біржі, обмінні ресурси або інші електронні гаманці, у т.ч. з використанням так званих "міксерів", які унеможливлюють відстеження подальшого руху криптовалюти;

3) різного роду шахрайські схеми, внаслідок яких особи, які придбали криптовалюту, позбуваються її, відправляючи на гаманці зловмисників, або залишаються з нікому не потрібною криптовалютою, яка нічого не варта і яку неможливо продати;

а) добровільний переказ криптовалюти на шахрайську платформу, після чого особа втрачає доступ до неї і або внаслідок того, що за допомогою програмного забезпечення вартість її активів стає рівною нулю або просто одержувачі криптовалюти зникають із ввіреною криптовалютою;

в) втрата криптовалюти внаслідок фішингу, тобто інтернет-шахрайства, завдяки якому зловмисники отримують доступ до конфіденційних даних користувача – логіна і пароля від акаунта на біржі, або від електронного гаманця, на якому знаходиться криптовалюта. Зазвичай зловмисники відправляють потерпілому листа нібито від біржі чи гаманця, яким він користується, з проханням надати відповідну інформацію, щоб отримати доступ до акаунта, наприклад, з метою безпеки чи у зв'язку з тим, що обліковий запис скомпрометовано і він став відомий стороннім особам тощо;

г) злам комп'ютера чи смартфона, коли внаслідок шкідливого програмного забезпечення, спрямованого на крадіжку криптовалюти, інформація щодо криптовалютних гаманців та приватних ключів до них надсилається зловмисникам;

д) скам (у перекладі з норвезької – сором), тобто продаж нової криптовалюти або токена, вартість яких умисно "розганяється" зловмисниками, якими у проєкт вкладаються навіть мільйони доларів, і ціна швидко зростає; через соціальні мережі до проєкту залучаються все більше і більше учасників, коли ціна досягає певної величини, зловмисники продають за значну ціну всю криптовалюту, одержуючи надприбутки, а у покупців залишається нікому не потрібна криптовалюта чи токен, які нічого не варті і їх неможливо продати;

е) створення шахраями криптовалюти або токена зі схожою або й ідентичною назвою до монети, яка існує реально і має деякі перспективи, але ще не представлена на централізованих біржах. Її рекламують у соціальних мережах, але посилання надають на створену копію, у результаті інвестори купують клон, який нічого не вартий.

DOI (Article): https: //doi.org/10.36486/np.2022.4(58).17

DOI (Issue): https: //doi.org/10.36486/np.2022.4(58) Issue 4(58) 2022

Передусім при розслідуванні незаконного заволодіння криптовалютою слід враховувати тип активу, яким незаконно заволоділи. Адже у випадку, якщо має місце незаконне заволодіння криптовалютою, яка є централізованою, то найперше, що необхідно зробити – це звернутися до компанії-емітента криптовалюти із запитом щодо блокування викраденої криптовалюти у блокчейні з тим, щоб злочинець не зміг нею скористатися і в подальшому для можливості її арешту та повернення потерпілому.

Другою важливою обставиною, яку необхідно з'ясувати, є те, на який електронний гаманець виведено викрадені кошти: на власний зловмисника чи на гаманець біржі. Навіть за відсутності відповідної інформації може бути результативним звернення з відповідними запитами до найбільших бірж щодо одержання даних про те, чи не саме цій біржі належить електронний гаманець, і якщо так, то далі слід з'ясовувати, кому належить акаунт, з яких IP адрес здійснювалися входи в нього, а також, які ще криптовалюти на ньому зберігаються. Також необхідно вказувати у запиті про блокування акаунта та криптовалюти, яка на ньому знаходиться. Слід враховувати, що відповідно до вимог КПК України слідчий не наділений правом блокування криптовалюти на рахунку онлайн-біржі або емітента стейблкоїнів за відсутності судового рішення. Тому наступним кроком у процесі розслідування є звернення до слідчого судді з клопотанням про накладення арешту на акаунт та криптовалюту, яка на ньому знаходиться. Разом з тим, дієвих механізмів виконання ухвали слідчого судді наразі не існує, його направлення до криптовалютні біржі принесе результат, якщо біржа визнає таке блокування можливим та необхідним. Більше того, зазвичай біржі знаходяться у різних юрисдикціях і фактично рішення слідчого судді в Україні де-юре не є обов'язковим для виконання наприклад, у Японії, на Мальті або в Канаді чи на Віргінських островах.

Наприклад, найбільша криптовалютна біржа світу Binance надає доступ до "Системи для здійснення запитів державними та правоохоронними органами (LERS)". Щоб отримати доступ до LERS, агент правоохоронних органів або державний службовець повинен спочатку здійснити запит на доступ. Зазвичай запит на доступ розглядається та затверджується упродовж трьох робочих днів, після чого правоохоронці можуть здійснити запит на інформацію та завантажити відповідні підтверджуючі документи. Щоб Binance могла надати інформацію про користувачів у межах поточного кримінального розслідування, потрібна чинна судова постанова від компетентної юрисдикції або постанова/розпорядження від поліції [8].

Якщо під час огляду чи обшуку слідчий виявляє апаратний криптовалютний гаманець, то мають бути вжиті заходи до знаходження паролю від нього. Те саме стосується і смартфонів, планшетів та ноутбуків зловмисників. І тут все можуть вирішувати хвилини або навіть секунди, адже доступ до криптовалютних гаманців можуть мати спільники вказаних вище осіб і будь-яка повільність у вжитті заходів щодо переведення виявленої криптовалюти на криптовалютні гаманці, які контролюються органом досудового розслідування може мати фатальні наслідки, адже спільникам достатньо кількох хвилин для того, щоб перевести криптовалюту із одного електронного гаманця на інший.

DOI (Article): https: //doi.org/10.36486/np.2022.4(58).17

У протоколах огляду, обшуку мають бути чітко зазначені такі дані: назва криптовалюти, її кількість, дані електронних гаманців, на яких вона знаходиться, назви логіну чи облікового запису, на якій криптовалюта знаходиться, паролі доступу до нього та ідентифікатори нових електронних гаманців органів досудового розслідування, на які криптовалюту переведено, якщо таке мало місце. Крім того, у протоколах, залежно від конкретних обставин та особливостей гаманців і блокчейнів, за умови технічної можливості, мають бути вказані хеші транзакцій та час їх проведення, ідентифікатори гаманців, з яких та на які проводилися транзакції. При цьому для слідчих (розшукових дій) вкрай важливим є залучення, відповідно до вимог ст. 71 КПК України, спеціалістів у сфері ІТ та криптовалют.

Зазвичай прийнято вважати, що будь-яка криптовалюта є анонімною і встановити особу, якій вона належить, неможливо. Проте визначальним є те, що будь-яка транзакція записується в блокчейні і зберігається там назавжди. Це означає, якщо біткоїн чи інша криптовалюта побувала в електронному гаманці, який пов'язують зі злочинною діяльністю певної особи або групи осіб, то скільки б разів і на які інші адреси гаманців потім криптовалюту не пересилали, приховати інформацію про це не вдасться, адже в будь-який час можна вільно переглянути дані блокчейну та побачити всі транзакції за відповідною адресою.

Крім того, для аналізу блокчейнів можна використовувати можливості спеціалізованих сервісів. Так, проведений В.В Носовим та І.А. Манжай аналіз засвідчив, що серед інструментів аналізу в роботі правоохоронних органів також можна застосовувати: bitconeview.info – для візуалізації трансакцій; github.com/mikispag/bitiodine – для аналізу біткоїн блокчейну з можливістю кластеризації; github.com/BitcoinOpReturn/OpReturnTool – для вилучення OP_RETURN метаданих з біткоїн блокчейну; blockchain.info – для швидкого виконання базових функцій аналізу трансакцій; anyblockanalytics.com – для аналізу руху різних криптовалют; Chainalysis, Elliptic, Ciphertrace, Blockchain Inspector – для аналізу ризиків, пов'язаних із біткоїн-трансакціями [9, с. 96].

Але це не стосується анонімних криптовалют, транзакції яких у блокчейні відстежити неможливо, або досить складно – Monero, Zcash, Komodo, Horizen (Zencash), Verge, PIVX та низки інших.

Також серед злочинців користуються популярністю так звані "міксери", тобто онлайн-сервіси, що дозволяють користувачам змішувати свої цифрові активи з активами інших користувачів. Після переказу коштів через міксер ніхто й ніколи не дізнається звідки і хто їх перерахував, оскільки сервіс приховує зв'язок між відправником та одержувачем.

Tornado Cash став найпопулярнішим інструментом для відмивання коштів серед хакерів – на совісті та рахунках зловмисників опинились мільярди доларів, які повернути неможливо. Щоб боротися з хакерами, уряд США вирішив заборонити криптовалютний міксер. Так 8 серпня 2022 року у США запровадили санкції, що забороняють громадянам і підприємствам Америки користуватися послугами Tornado Cash. Після запровадження таких заборон криптоплатформи масово почали блокувати адреси, пов'язані з міксером. Через кілька днів після запровадження санкцій розробника Tornado Cash Алєксєя Перцева затримали в

DOI (Article): https: //doi.org/10.36486/np.2022.4(58).17

Амстердамі й одразу доставили до суду, висунувши обвинувачення у відмиванні вкрадених криптовалют та співпраці зі зловмисниками [10].

Важливе правило розслідування – йти за "цифровим слідом", яким є адреси електронних гаманців із транзакціями та будь-які інші дані, добуті в ході досудового розслідування: IP-адреси входу на біржі чи електронні гаманці, електронні адреси та номери телефонів, пов'язані з акаунтами тощо, що і дозволить зрештою встановити особу злочинця, затримати його і повернути викрадену криптовалюту її законному власнику.

Яскравим прикладом цьому є останні результати розслідування крадіжки століття у світі криптовалют. Міністерство юстиції США оголосило про розкриття найбільшої в історії крадіжки криптовалюти, конфіскувавши біткойни на рекордну суму в $3,6 мільярда у подружжя, яке, ймовірно, зламало в 2016 році криптовалютну біржу Bitfinex. Заарештована у цій справі подружня пара – 34-річний Ілля Ліхтенштейн та 31-річна Хізер Морган були заарештовані у Манхеттені і постали перед судом, повідомляє Голос Америки. Їм висунуті звинувачення у вступі в змову з метою відмивання грошей, а також в обмані влади. За словами заступника генерального прокурора США Лізи Монако, затримані стоять за найбільшим в історії фінансовим розкраданням. Заступник генпрокурора США також наголосила, що успішна операція, проведена Мінюстом, стала доказом того, що криптовалюта більше "не є притулком для злочинців". Подружню пару звинувачують у відмиванні 119 754 біткойнів, вкрадених внаслідок хакерського злому криптовалютної біржі Bitfinex. Представники Міністерства юстиції заявили, що на момент скоєння злочину вартість викрадених коштів оцінювалася у $71 млн у біткойнах, однак, з урахуванням зростання вартості криптовалюти, зараз обсяг вкрадених біткойнів оцінюється у більш ніж $4,5 млрд. За даними слідства, Ліхтенштейн і його дружина також намагалися відмивати гроші через мережу обмінних пунктів і проводили кошти як платежі стартап-компанії, відкритої Хізер Морган. У подальшому незаконні доходи були витрачені на придбання різних речей – починаючи із золота та NFC-токенів та закінчуючи "абсолютно приземленими" – подарунковими сертифікатами торгової мережі Walmart. Ключовою подією у розслідуванні цього злочину міг стати крах підпільного даркнет-ринку AlphaBay, який припинив існування у 2017 році внаслідок дій правоохоронних органів. У Мінюсті повідомили, що частину викрадених хакерами коштів було переведено на AlphaBay. За даними компанії Elliptic, що займається відстеженням цифрової валюти, закриття нелегального сайту, ймовірно, дозволило владі отримати доступ до внутрішніх транзакцій AlphaBay і пов'язати їх із криптовалютним рахунком, відкритим на ім'я Ліхтенштейна [11].

Іншим слабким місцем будь-якого злочину, пов'язаного з незаконним заволодінням криптовалютою, є те, що викрадену криптовалюту злочинцям зрештою захочеться обміняти на грошові кошти, і в окремих випадках це може бути зроблено, наприклад, із біржі на номер банківського рахунку або номер банківської карти, які належать конкретній фізичній особі, тому з'ясування відповідних даних може допомогти у затриманні злочинців навіть у випадку, якщо останні використовують TOR та VPN для того, щоб анонімізувати IP адреси та зашифрувати свої інтернет-підключення з метою приховування їх діяльності в мережі Інтернет для того, щоб їх неможливо було відстежити.

Так, браузер Tor є тандемом сучасної версії Mozilla Firefox і програмного забезпечення з акцентом на приватність. Програма є безкоштовною, дозволяє ефективно обходити цензуру в мережі. Мережа браузера складається з безлічі серверів, розкиданих по всьому світу, якими керують волонтери. Анонімність забезпечується шляхом з'єднання з трьома ретрансляторами, кожен з яких є зашифрованим. У результаті обчислити шлях руху інформації від одержувача до відправника стає неможливо.

При використанні TOR задіюється інша IP-адреса, яка часто належить іншій країні. При цьому IP-адреса є прихованою від сайтів, які відвідує користувач. Додатковим заходом безпеки є шифровка відвідуваних сайтів від сторонніх осіб, які можуть перехопити рух трафіка. Це зводить ризик стеження онлайн до нуля. Так само TOR дозволяє обходити інтернет-фільтри. Користувачеві стають доступні сайти та ресурси, які раніше були недоступні через блокування всередині країни [12].

Іншою технологією, яка дозволяє анонімізувати свою діяльність у мережі Інтернет, є VPN (Virtual Private Network) – це віртуальна приватна мережа, яка забезпечує шифрування трафіка між клієнтом та VPN-сервером і зміну IP-адреси. При підключенні до VPN створюється захищений канал між комп'ютером користувача і VPN-сервером. Дані в ньому надійно зашифровані: ваш інтернет-провайдер не дізнається вашої локації та вебресурсів, які ви відвідали. Оновлена IP-адреса зазвичай створюється з іншого міста або країни. Наприклад, ви можете увійти в систему з Києва, перебуваючи в Україні, але ваша IP-адреса буде вказувати, що Ви, наприклад, у Лондоні, Великій Британії. VPN-сервіси дозволяють користуватися ресурсами, доступ до яких заборонено за географічним принципом або на підставі рішень органів влади. Завдяки VPN можна вільно відвідувати заблоковані сайти, достатньо лише вибрати та завантажити додаток на свій комп'ютер або мобільний пристрій [13].

Хрестоматійним прикладом встановлення особи злочинця у сфері незаконного обігу криптовалют є історія про затримання ФБР засновника Silk Road (з англ. шовковий шлях) – анонімного інтернет-магазину, який перебував у доменній зоні .onion анонімної мережі Tor. Більшість товарів, виставлених на сайті, були наркотичними речовинами. Розрахунок за придбаний товар здійснювався за допомогою криптовалюти Bitcoin, яка забезпечує високий ступінь анонімності [13].

Ним виявився Росс Ульбріхт. Встановити його особу вдалося завдяки співробітнику податкового управління США Елфорду, який здогадався, що засновник Silk Road мав би розкручувати майданчик на сайтах зі схожою аудиторією. Він відшукав посилання на IP-адреси Tor часів Silk Road і знайшов, що 27 січня 2011 року на сайті Shroomery.org дехто Altoid рекламував новий майданчик для анонімної купівлі та продажу будь-яких товарів.

Простий пошук в Google за ніком Altoid привів на сайт Stack Overflow. На ньому особа з поштою rossulbricht@gmail.com цікавилася технічними особливостями Tor. Пошук у базах ФБР показав, що Росс Ульбріхт завжди знаходився поблизу від місць виходу Жахливого пірата Робертса (нік власника Silk Road) в Silk Road [14].

DOI (Article): https: //doi.org/10.36486/np.2022.4(58).17

Отже, дослідивши основи розслідування злочинів щодо незаконного заволодіння криптовалютою, доходимо до висновків про важливість знань видів криптовалют та особливостей функціонування їх блокчейнів, а також уміння аналізувати блокчейни, у тому числі із застосуванням можливостей спеціальних сервісів. Так само важливо до проведення слідчих (розшукових дій) залучати, відповідно до вимог ст. 71 КПК України, спеціалістів у сфері ІТ та криптовалют. Ключовим є встановлення електронного гаманця, на який виведено викрадену криптовалюту та співпраця з біржами для одержання даних про те, кому належить акаунт, з яких IP-адрес здійснювалися входи в нього та які ще криптовалюти на ньому зберігаються. У запиті слід вказувати також про блокування акаунта та криптовалюти, яка на ньому знаходиться. Надалі слід звертатися до слідчого судді з клопотанням про арешт криптовалюти. Під час розслідування необхідно йти за "цифровим слідом", яким є адреси електронних гаманців із транзакціями та будь-які інші дані: IP-адреси входу на біржі чи електронні гаманці, електронні адреси та номери телефонів, пов'язані з акаунтами, банківські карти, на які зараховувалися грошові кошти, отримані від продажу криптовалюти тощо, це дозволить зрештою встановити особу злочинця, затримати його і повернути викрадену криптовалюту її законному власнику. Успіх розслідування також залежить від того, чи використовували злочинці анонімні криптовалюти, які практично неможливо відстежити, та міксери криптовалют, а також сервіси TOR та VPN при створенні криптовалютних гаманців і при заволодінні криптовалютою тощо, але будь-яка найменша допущена ними помилка може стати запорукою успішного розкриття злочину.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Reuters. FTX to start U.S. bankruptcy proceedings, CEO to exit. URL: https://www.reuters.com/business/ftx-scrambles-funds-regulators-take-action-2022-11-11 (дата звернення: 09.10.2022).

2. Bloomberg. FTX Latest: Police Consider Criminal Probe. URL: https://www.bloomberg.com/news/articles/2022-11-12/ftx-latest-unauthorized-outflows-bankman-fried-in-the-bahamas?srnd=premium-europe (дата звернення: 09.10.2022).

3. Noworries. Криптовалютна біржа Kraken дізналася ім'я хакера, що вкрав $ 600 мільйонів у FTX. URL: https://noworries.news/kryptovalyutna-birzha-kraken-diznalasya-imya-hakera-shho-vkrav-600-miljoniv-u-ftx (дата звернення: 09.10.2022).

4. CoinmarketCap. URL: https://coinmarketcap.com (дата звернення: 09.10.2022).

5. Криптовалютний Сальвадор: як біткоїн уперше став національною валютою. URL: https://mind.ua/publications/20230885-kriptovalyutnij-salvador-yak-bitkoyin-upershe-stav-nacionalnoyu-valyutoyu (дата звернення: 09.10.2022).

6. *Логойда В.М.* Правовий статус криптовалюти в країнах Африки. *Закарпатські правові читання. Трансформація національних правових систем країн Центральної та Східної Європи в умовах сучасних викликів*: матеріали XIV міжнародної науково-практичної конференції, м. Ужгород, 28–29 квітня 2022 р. Ужгород: Видавничий дім "Гельветика", 2022. С. 262–265.

7. Про віртуальні активи: Закон України від 17 лютого 2022 року № 2074-IX. офіц. текст / офіційний вебсайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text (дата звернення: 09.10.2022).

8. Binance. Система для здійснення запитів державними та правоохоронними органами (LERS). URL: https://www.binance.com/uk-UA/support/law-enforcement. (дата звернення: 09.10.2022).

9. *Носов В.В., Манжай І.А.* Окремі аспекти аналізу криптовалютних трансакцій під час попередження та розслідування злочинів. *Право і безпека*. 2021. № 1 (80). С. 93–100.

10. Криптовалютні міксери: допомога хакерам чи бажання свободи. URL: https://noworries.news/kryptovalyutni-miksery-dopomoga-hakeram-chy-bazhannya-svobody (дата звернення: 09.10.2022).

DOI (Issue): https: //doi.org/10.36486/np.2022.4(58) Issue 4(58) 2022

11. Бізнес Цензор. Мінюст США знайшов вкрадені біткойни на рекордні $3,6 мільярда. URL:https://biz.censor.net/news/3315121/minyust_ssha_znayishov_vkradeni_bitkoyiny_na_rekordni_36_milyarda (дата звернення: 09.10.2022).

12. ІЩо таке TOR браузер? Як його налаштувати і користуватися. URL: https://wifi-help.net/chto-takoe-tor-brauzer-kak-ego-nastroit-i-polzovatsya (дата звернення: 09.10.2022).

13. ІЩо таке VPN, і як ним безпечно користуватись / офіційний вебсайт Державної служ би спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua/news/sho-take-vpn-i-yak-nim-bezpechno-koristuvatis (дата звернення: 09.10.2022).

14. Silk Road. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Silk_Road (дата звернення: 09.10.2022).

REFERENCES

1. Reuters. FTX to start U.S. bankruptcy proceedings, CEO to exit URL: https://www.reuters.com/business/ftx-scrambles-funds-regulators-take-action-2022-11-11 (Date of Application: 09.10.2022) [In English].

2. Vloomberg. FTX Latest: Police Consider Criminal Probe URL: https://www.bloomberg.com/news/articles/2022-11-12/ftx-latest-unauthorized-outflows-bankman-fried-in-the-bahamas?srnd=premium-europe (Date of Application: 09.10.2022) [In English].

3. Noworries. Kryptovaliutna birzha Kraken diznalasia imia khakera, shcho vkrav $ 600 milioniv u FTX. "Cryptocurrency exchange Kraken has learned the name of the hacker who stole $600 million from FTX". URL: https://noworries.news/kryptovalyutna-birzha-kraken-diznalasya-imya-hakera-shho-vkrav-600-miljoniv-u-ftx (Date of Application: 09.10.2022) [In Ukrainian].

4. SoinmarketSap URL: https://coinmarketcap.com (Date of Application: 09.10.2022) [In English].

5. Kryptovaliutnyi Salvador: yak bitkoin upershe stav natsionalnoiu valiutoiu. "Cryptocurrency El Salvador: How Bitcoin Became a National Currency for the First Time". URL: https://mind.ua/publications/20230885-kriptovalyutnij-salvador-yak-bitkoyin-upershe-stav-nacionalnoyu-valyutoyu (Date of Application: 09.10.2022) [In Ukrainian].

6. *Lohoida V.M.* (2022). Pravovyi status kryptovaliuty v krainakh Afryky. "Legal status of cryptocurrency in African countries". Zakarpatski pravovi chytannia. Transformatsiia natsionalnykh pravovykh system krain Tsentralnoi ta Skhidnoi Yevropy v umovakh suchasnykh vyklykiv. "Transcarpathian legal readings. Transformation of the national legal systems of the countries of Central and Eastern Europe in the conditions of modern challenges". Uzhhorod: Vydavnychyi dim "Helvetyka". P. 262–265 [In Ukrainian].

7. Pro virtualni aktyvy. "About virtual assets": Law of Ukraine dated February 17, 2022 No. 2074-IX. officer text: veb-sait Verkhovnoi Rady Ukrainy. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text (Date of Application: 09.10.2022) [In Ukrainian].

8. Binance. Systema dlia zdiisnennia zapytiv derzhavnymy ta pravookhoronnymy orhanamy (LERS). "State and Law Enforcement Inquiries System (LERS)". URL: https://www.binance.com/uk-UA/support/law-enforcement (Date of Application: 09.10.2022) [In Ukrainian].

9. *Nosov V.V., Manzhai I.A.* (2021). Okremi aspekty analizu kryptovaliutnykh transaktsii pid chas poperedzhennia ta rozsliduvannia zlochyniv. "Certain aspects of the analysis of cryptocurrency transactions during the prevention and investigation of crimes". Law and security. No. 1 (80). P. 93–100 [In Ukrainian].

10. Kryptovaliutni miksery: dopomoha khakeram chy bazhannia svobody. "Cryptocurrency mixers: helping hackers or wanting freedom". URL: https://noworries.news/kryptovalyutni-miksery-dopomoga-hakeram-chy-bazhannya-svobody (Date of Application: 09.10.2022) [In Ukrainian].

11. Biznes Tsenzor. Miniust SShA znaishov vkradeni bitkoiny na rekordni $3,6 miliarda. "Business Censor. The US Department of Justice found stolen bitcoins worth a record $3.6 billion. URL: https://biz.censor.net/news/3315121/minyust_ssha_znayishov_vkradeni_bitkoyiny_na_rekordni_36_milyarda (Date of Application: 09.10.2022) [In Ukrainian].

12. Shcho take TOR brauzer? Yak yoho nalashtuvaty i korystuvatysia. "What is the TOR browser? How to set it up and use it". URL: https://wifi-help.net/chto-takoe-tor-brauzer-kak-ego-nastroit-i-polzovatsya (Date of Application: 09.10.2022) [In Ukrainian].

13. Shcho take VPN, i yak nym bezpechno korystuvatys. "What is a VPN and how to use it safely: Official website of the State Service for Special Communications and Information Protection.

DOI (Article): https: //doi.org/10.36486/np.2022.4(58).17

URL: https://cip.gov.ua/ua/news/sho-take-vpn-i-yak-nim-bezpechno-koristuvatis (Date of Application: 09.10.2022) [In Ukrainian].

14. *Silk Road*. Vikipediia URL: https://uk.wikipedia.org/wiki/Silk_Road (Date of Application: 09.10.2022) [In English].

UDC 343.13

Movchan Anatolii,
Doctor of Juridical Sciences, Full Professor, Professor of the Department,
Lviv State University of Internal Affairs, Lviv, Ukraine,
ORCID ID 0000-0002-6997-6517
Kozii Vasyl,
Candidate of Juridical Sciences, Doctoral student,
Lviv State University of Internal Affairs, Lviv, Ukraine,
ORCID ID 0000-0002-8221-6678

FUNDAMENTALS OF INVESTIGATION CRIMES REGARDING ILLEGAL POSSESSION OF CRYPTOCURRENCY

The article is devoted to the study of the fundamentals of the investigation of crimes related to the illegal possession of cryptocurrency.

The purpose of this article is to determine the basics of the investigation of crimes related to illegal possession of cryptocurrency, and to find ways to solve them. Dialectical, comparative-legal, systemic-structural, and formal-logical methods were used to achieve the goal. The concept of cryptocurrency and the peculiarities of its circulation and functioning are analyzed, problematic issues of the investigation of crimes related to the illegal acquisition of cryptocurrency are identified, which are subject to resolution both at the scientific level and in the practical activities of investigative bodies of pre-trial investigation and prosecutors. The main methods of committing crimes of this category are defined and practical recommendations are formulated regarding the methodology and tactics of investigating the illegal possession of cryptocurrency. Emphasis is placed on the need to know the peculiarities of the functioning of cryptocurrency blockchains, to use their analysis. Specialists in the field of cryptocurrencies should be involved in the investigation. The importance of cooperation with cryptocurrency exchanges for the seizure of stolen cryptocurrencies was noted. It shows the problems of investigating the theft of anonymous cryptocurrencies, the use of cryptocurrency mixers by criminals, as well as Tor and VPN services.

The importance of establishing during the investigation the addresses of electronic wallets with transactions, the IP addresses from which the exchanges or electronic wallets were entered, the phone numbers associated with the accounts, the bank card numbers to which the money received from the sale of cryptocurrency was received was also emphasized.

Keywords: cryptocurrency, pretrial investigation, crimes in the field of cryptocurrencies, blockchain, illegal possession of cryptocurrency, investigation of illegal possession of cryptocurrency.

Отримано 02.12.2022