особисто. Це вказує на можливість використання кримінального аналізу та його результатів не тільки оперативними підрозділами Національної поліції. Враховуючи специфіку протидії оперативними підрозділами кримінальним правопорушенням за допомогою негласних позаштатних працівників в умовах правового режиму воєнного стану, роль такої можливості в процесі вказаної протидії може бути незамінною.

Підсумовуючи, зазначимо, що в наш час спостерігається активний розвиток цифрового суспільства, соціальних мереж, месенджерів тощо. Використання оперативними підрозділами під час протидії кримінальним правопорушенням за допомогою негласних позаштатних працівників вище перелічених інструментів кримінального аналізу є необхідністю.

УДК 343.14
DOI: 10.31733/17-03-2023-384-387

Василь КОЗІЙ
докторант кафедри
оперативно-розшукової діяльності
Львівського державного
університету внутрішніх справ,
кандидат юридичних наук

ОКРЕМІ АСПЕКТИ ДОКАЗУВАННЯ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ ПРО ЗЛОЧИНИ ЩОДО НЕЗАКОННОГО ЗАВОЛОДІННЯ КРИПТОВАЛЮТОЮ

Починаючи із 2008 року – із появи першої у світі криптовалюти – біткоїна, і по теперішній час у світі відбувся бурхливий розвиток криптовалют. Тепер це ціла індустрія: у мережі інтернет тисячі ресурсів надають можливості будь-кому всього за кілька хвилин за допомогою грошових коштів із банківської карти стати власником однієї чи кількох із багатьох тисяч криптовалют. Так, наприклад, на ресурсі Coin Geko станом на 02.03.2032 рік містилася інформація про 12 309 монет, і це далеко не всі, а лише ті, які вказаний ресурс відстежує [1].

Однією із нагальних потреб і вимог часу є запровадження прозорого і чіткого контролю за діяльністю на ринку криптовалют. Регулятори багатьох країн намагаються законодавчо впорядкувати правила їх обігу. Загалом для надання послуг користувачам тієї чи іншої країни уряди запроваджують правила для криптовалютних бірж та обмінників, відповідно до яких оператори таких бірж повинні отримати ліцензії на здійснення відповідної діяльності. При цьому криптовалюту розглядають як активи, торгівля та обмін якими підлягають оподаткуванню.

В Україні криптовалюту на законодавчому рівні віднесено до віртуальних активів. Більше року тому, 17.02.2022 ухвалено Закон України «Про віртуальні активи», який проте до цього часу не набрав чинності. Згідно з п. 1 указаного Закону 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 [2].

Із року в рік правоохоронці у всьому світі все частіше й частіше стикаються із фактами незаконного заволодіння криптовалютою. Не є винятком і Україна. Крім викрадення криптовалюти різними способами, (злами криптовалютних бірж, електронних гаманців, різні шахрайські схеми і т. ін.) злочинці її також у багатьох випадках використовують для легалізації незаконно здобутого майна, продажу та придбання зброї, наркотичних та психотропних речовин, а також для фінансування тероризму.

Наприклад, за процесуального керівництва Офісу Генерального прокурора здійснюється досудове розслідуванням у кримінальному провадженні за фактом фінансування тероризму (ч. 3 ст. 258-5 КК України). За даними слідства, з травня 2022 року в окремих регіонах України у змові з представниками псевдореспублік «Л/ДНР» діяла група осіб, яка займалася фінансовими махінаціями. Їх метою було заволодіння грошовими

коштами, які знаходилися на банківських рахунках громадян України на тимчасово окупованих територіях, зокрема Донецької та Луганської областей. В подальшому ці кошти через криптобіржі перераховувались, у тому числі представникам «Л/ДНР». Гроші використовувалися в інтересах учасників терористичних організацій для нанесення шкоди національній безпеці України. В рамках розслідування кримінального провадження було проведено

27 обшуків. Вилучено речові докази, що підтверджують злочинну діяльність. Також накладено арешти на криптоактиви в розмірі 65 млн грн. Досудове розслідування здійснюється слідчими Головного слідчого управління СБУ. Оперативний супровід – Департамент захисту національної державності СБУ [3].

Відповідно до даних експертів з кібербезпеки PeckShield упродовж лютого 2023 року зловмисники поцупили $ 35,3 млн у криптоактивах. Фахівці зафіксували понад 200 експлойтів. При цьому 141 злам стався в один день – 11 лютого. Найбільшу суму – $ 9,2 млн. – хакери викрали внаслідок атаки на користувачів гаманців MyAlgo. За ним за обсягом вкрадених коштів слідує DeFi-протокол Platypus. У PeckShield зазначили, що в ході зламу протоколу BonqDAO зловмисники намагалися викрасти близько $ 120 млн, але змогли вивести тільки $ 2 млн. Станом на 28 лютого хакери переказали частину коштів до міксеру Tornado Cash. Зокрема, аналітики ідентифікували транзакції на понад 9 000 ETH і 6 000 BNB [4].

Ці та інші випадки незаконного заволодіння криптовалютою потребують пильної уваги правоохоронців, слідчих, детективів та оперативних працівників і обвинувальні акти щодо винних осіб повинні направлятися до суду та розглядатися по суті в розумні строки. Отже у кримінальних провадженнях цієї категорії актуальним є визначення особливостей доказування.

Відповідно до вимог ч. 1 ст. 91 КПК України у кримінальному провадженні підлягають доказуванню:

1) подія кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення);

2) винуватість обвинуваченого у вчиненні кримінального правопорушення, форма вини, мотив і мета вчинення кримінального правопорушення;

3) вид і розмір шкоди, завданої кримінальним правопорушенням, а також розмір процесуальних витрат;

4) обставини, які впливають на ступінь тяжкості вчиненого кримінального правопорушення, характеризують особу обвинуваченого, обтяжують чи пом'якшують покарання, які виключають кримінальну відповідальність або є підставою закриття кримінального провадження;

5) обставини, що є підставою для звільнення від кримінальної відповідальності або покарання;

6) обставини, які підтверджують, що гроші, цінності та інше майно, які підлягають спеціальній конфіскації, одержані внаслідок вчинення кримінального правопорушення та/або є доходами від такого майна, або призначалися (використовувалися) для схиляння особи до вчинення кримінального правопорушення, фінансування та/або матеріального забезпечення кримінального правопорушення чи винагороди за його вчинення, або є предметом кримінального правопорушення, у тому числі пов'язаного з їх незаконним обігом, або підшукані, виготовлені, пристосовані або використані як засоби чи знаряддя вчинення кримінального правопорушення [5].

Ці обставини є загальними для будь-яких кримінальних правопорушень. Проте у кримінальних провадженнях про незаконне заволодіння криптовалютою є певні особливості, з огляду на специфіку таких злочинів.

Передусім слід враховувати, що при описі способу вчинення злочину у багатьох випадках необхідним є дотримання контекстуального підходу.

І тут найближчу схожість і певні паралелі можна провести із злочинами, вчиненими в умовах збройного конфлікту. Так, дослідження значення контекстуальних обставин як елементів складу злочину при розслідуванні окремих категорій злочинів дозволило Г. Тетерятник дійти висновків про те що необхідним є доктринальне дослідження контекстуальних обставин вчинення кримінальних правопорушень та їх вплив на кримінальну кваліфікацію в межах вітчизняного правового поля в умовах збройного конфлікту, виділення спеціального предмету доказування по таким кримінальним правопорушенням, визначення спеціальних механізмів доказування. Перспективними

вбачаються подальші наукові розвідки з питань з'ясування поняття, правової природи, значення контекстуальних обставин як елементів кримінального правопорушення та їх вплив на здійснення процесу доказування у кримінальних провадженнях в умовах надзвичайних правових режимів [6, с. 249].

Контекстуальними обставинами у кримінальних провадженнях про злочини щодо незаконного заволодіння криптовалютою, залежно від конкретних обставин, можуть бути: особливості функціонування тієї чи іншої криптовалюти, тобто опис того, як функціонує блокчейн та яким чином здійснюються транзакції; яке програмне та апаратне забезпечення потрібно для здійснення транзакцій; як відбувається торгівля та обмін криптовалюти на тій чи іншій централізованій або децентралізованій біржі та які засоби безпеки запроваджено; яким чином працюють смарт-контракти; яка історія торгів на визначеній біржі з визначеного акаунта упродовж визначеного часу, з яких IP та ін. Також це може бути загальна інформація про індустрію криптовалют в цілому. Наприклад, якщо йдеться про крах або злам криптовалютної біржі, то до контекстуальних обставин можуть відноситися дані про те хто і коли її заснував, у яких юрисдикціях вона зареєстрована, як організовано її роботу, які показники такої роботи, як здійснювалося керівництво біржею, які попередні «схожі за почерком» спроби передували зламу.

Іншою, не менш важливою особливістю є те, що будь-які докази, які подаються в суді мають пояснюватися простою та зрозумілою мовою для осіб, які не фахівцями в індустрії криптовалют. Це стосується технічних особливостей функціонування тієї чи іншої криптовалюти, технічних особливостей функціонування криптовалютних бірж, способів верифікації користувачів на біржах, особливостей функціонування програмного забезпечення для зберігання криптовалют і т. ін.

Надзвичайно важливою є необхідність пояснення того, про що свідчать ті чи інші факти, які обставини вони підтверджують або спростовують у своїй сукупності. У цьому контексті показовим є звіт агента ФБР про те, яким чином було встановлено особу власника даркнет маркетплейсу Silk Road Росса Ульбіхта, відомого як «Dread Pirate Roberts». Зокрема у параграфі 39 звіту агентом відзначено: «Згідно із записами про користувача одержаним за допомогою Google, Gmail аккаунт Ульбріхта зареєстровано на ім'я «Росс Ульбріхт». Записи свідчать про те, що Ульбріхт має акаунт в Google+, сервісі соціальної мережі Google. Після вивчення публічно доступного профілю Ульбріхта на Google+, я з'ясував, що він містить його фото, яке відповідає фото у профілі «Росс Ульбріхт» на LinkedIn, як про це згадується в параграфі 33…41. Розслідування також підтвердило той факт, що на початку червня 2013 року Ульбріхт проживав у Сан-Франциско, Каліфорнія, поряд з інтернет-кафе, із якого встановлювалося з'єднання із сервером, який використовувався для адміністрування Silk Road. А саме:

Мною вивчено записи, одержані від Google, які містять в логах IP адреси, з яких здійснювався вхід в Gmail акаунт Ульбріхта з 13.01.2013 р. по 20.06.2013 р. IP логи свідчать, що упродовж цього часу до акаунту регулярно здійснювався доступ з визначеної IP адреси Comcast. Згідно з записами одержаними від Comcast, вказана IP адреса у вказаний час доступу була зареєстрована за визначеною адресою по вул. Хікорі, Сан-Франциско, Каліфорнія. За цією адресою зареєстрована інша особа, яка, як мені відомо, є другом Ульбріхта, у якої він зупинився, коли приїхав до Сан-Франциско орієнтовно у вересні 2012 року, що підтверджується відео, розміщеним на YouTube, на якому обоє друзів за обставин, які підтверджують ці міркування.

Ґрунтуючись на моєму дослідженні приватного листування DPR, відновленого з веб-сервера Silk Road, мені відомо, що DPR регулярно вказував Тихоокеанську тимчасову зону, коли оперував часом. Наприклад, в одному особистому повідомленні, датованому 18.04.2013 р. DPR повідомляє іншому користувачеві Silk Road: «Зараз приблизно 4 години дня за Тихоокеанським (стандартним) часом. Мені потрібно зайнятися деякими справами». Виходячи з моєї підготовки та досвіду, я вважаю, що ця тенденція говорить про те, що DPR фізично знаходиться в Тихоокеанській тимчасовій зоні, в якій, зрозуміло і знаходиться Сан-Франциско, Каліфорнія».

Як бачимо, агентом надається пояснення кожному факту та обставині, що має значення для справи.

Важливим у доказуванні, з урахуванням конкретних обставин вчинення злочину є зазначення і підтвердження доказами фактів, які свідчать про те, що підозрюваний чи обвинувачений в силу своєї освіти та наявності відповідних знань, а також умінь і навичок у сфері IT загалом та наприклад, конкретно програмування чи інженерії блокчейну міг

вчинити незаконне заволодіння криптовалютою. На підтвердження певних фактів можуть бути використані дані, які містяться в дипломах про освіту, сертифікати про закінчення відповідних курсів, проходження тренінгів, участь у тематичних заходах, дані із соціальних мереж, з яких слідує, що особа позиціонує себе причетною до певної спільноти. Очевидно, що прибиральник приміщень, який не обізнаний із сферою ІТ та у якого у користуванні навіть немає смартфона або іншого гаджета із програмним забезпеченням для торгівлі та зберігання криптовалют не здатний незаконно заволодіти криптовалютою і, відповідно, бути підозрюваним або обвинуваченим у цьому, якщо тільки немає доказів, які спростовують вищевказане.

Підбиваючи підсумки наведеному вище, слід відзначити, що доказування у кримінальних провадженнях про незаконне заволодіння криптовалютою має свої особливості, які полягають у тому, що при описі способу вчинення злочину у багатьох випадках є необхідним дотримання контекстуального підходу. Також будь-які докази, які подаються на підтвердження або спростування тих чи інших фактів або обставин мають пояснюватися простою та зрозумілою мовою для осіб, які не фахівцями в індустрії криптовалют. Крім того, важливим у доказуванні є доведення того, що підозрюваний чи обвинувачений в силу своєї освіти та наявності відповідних знань, а також умінь і навичок у сфері ІТ загалом та наприклад, конкретно програмування чи інженерії блокчейну міг вчинити незаконне заволодіння криптовалютою.

1. CoinGeko. URL: https://www.coingecko.com/uk.
2. Про віртуальні активи: Закон України від 17.02.2022 р. № 2074-IX. Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text.
3. Ліквідовано потужну фінансову схему допомоги псевдо республікам. URL: https://www.gp.gov.ua/ua/posts/likvidovano-potuznu-finansovu-sxemu-dopomogi-psevdorespublikam.
4. More than 200 exploits grabbed $ 35.3M in February 2023. URL: https://twitter.com/PeckShieldAlert.
5. Кримінальний Кодекс України: Закон України від 05.04.2001 р. № 2341-III. Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2341-14.
6. Тетерятник Г. К. Значення контекстуальних обставин як елементів складу злочину при розслідуванні окремих категорій злочинів. Права людини – пріоритет сучасної держави: зб. матер. конф. Всеукр. наук.-практ. Інтернет-конф. (м. Одеса, 10 грудня 2020 року). Одеса : Видавничий дім «Гельветика», 2020. С. 245-249.

УДК 343.14
DOI: 10.31733/17-03-2023-387-389

Юрій КРАМАРЕНКО
доцент кафедри
кримінально-правових дисциплін
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ОКРЕМІ ПИТАННЯ ФОРМУВАННЯ ГОТОВНОСТІ СПІВРОБІТНИКІВ ОПЕРАТИВНИХ ТА СЛІДЧИХ ПІДРОЗДІЛІВ ДО ПРОТИДІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ

Протидія злочинності, особливо її організованим формам, є одним із завдань правоохоронних органів. Результативність діяльності правоохоронних органів залежить від багатьох чинників серед яких можна виділити такі:

– компетентність співробітників правоохоронних органів, передусім слідчих та співробітників оперативних підрозділів;

– якість законодавства та правозастосування;

– стан розвитку та можливості удосконалення тактичних, технологічних та методологічних основ протидії злочинності;

– стан взаємодії між правоохоронними органами, іншими державними структурами та інститутами громадянського суспільства та можливості її удосконалення;