УДК 343.9
DOI https://doi.org/10.32782/2524-0374/2020-8/105

РОЗСЛІДУВАННЯ ЛЕГАЛІЗАЦІЇ (ВІДМИВАННЯ) ДОХОДІВ, ОТРИМАНИХ ЗЛОЧИННИМ ШЛЯХОМ ІЗ ВИКОРИСТАННЯМ ВІРТУАЛЬНИХ ВАЛЮТ (МЕТОДИЧНІ РЕКОМЕНДАЦІЇ)

INVESTIGATION OF THE LAUNDERING OF CRIME PROCEEDS USING VIRTUAL CURRENCIES (METHODOLOGY)

Кузьменко О.В., к.ю.н., доцент,
доцент кафедри кримінального процесу та криміналістики
Університет державної фіскальної служби України

Карпюк І.С., магістр кафедри кримінального процесу та криміналістики
Навчально-науковий інститут права
Університету державної фіскальної служби України

У статті розглянуто особливості методики розслідування легалізації (відмивання) доходів, отриманих злочинним шляхом із використанням віртуальних валют. Окремо визначено сучасний стан правового регулювання функціонування криптовалюти в Україні та міжнародні стандарти, до яких адаптовано національні норми права.

Також встановлено взаємозв'язок слідчої практики та положень спеціального законодавства, що стосується ринку віртуальних активів, та значення таких нормативних актів для правоохоронних органів.

Окремим питанням виділено роль віртуальних активів та можливість їх використання в процесі легалізації «брудних» коштів.

Також охарактеризовано характерні особливості вчинення легалізації доходів, отриманих злочинним шляхом за допомогою криптовалюти, на які необхідно звернути увагу в процесі розслідування, а саме: визначено основні групи критеріїв, які вказують на використання віртуальних валют у таких злочинах. Такі фактори поділено на дві групи: загальні, які застосовуються в багатьох методиках розслідування злочинів у кіберпросторі, та індикатори, що вказують на злочинну діяльність саме провайдерів віртуальних валют.

Досліджено інструменти та специфіку методології розслідування відмивання доходів, отриманих злочинним шляхом за допомогою віртуальних валют, особливості, які свідчать, що підозрюваний використовував у злочинній діяльності саме віртуальні активи. Особливу увагу приділено даним, що стосуються дослідження програмного забезпечення, яке необхідне для використання віртуальних активів та історії браузера, а також доказам, які можна отримати у процесі дослідження комп'ютера чи мобільного пристрою підозрюваного. Додатково виділено різноманітні категорії доказів, які можна отримати з комп'ютера особи, яка підозрюється в легалізації доходів, отриманих злочинним шляхом із використанням криптовалюти.

Проаналізовано обставини, які підлягають встановленню в процесі розслідування легалізації доходів, отриманих злочинним шляхом із використанням криптовалют, та докази, що підтверджують такі обставини.

Ключові слова: розслідування, легалізація (відмивання) доходів отриманих злочинним шляхом, віртуальні валюти, криптовалюта, провайдери віртуальних валют.

The article considers the peculiarities of the methodology of investigation of laundering of crime proceeds using virtual currencies. It draws the current state of legal regulation of cryptocurrency functioning in Ukraine and international standards in accordance with which national legal norms have been adapted.

The relationship between investigative practice and the provisions of special legislation concerning the virtual asset market and the significance of such regulations for law enforcement agencies have also been established.

A separate issue is the analysis the role of virtual assets and the possibility of their use in the process of legalization of "dirty" funds.

Also, the characteristic features of legalization of proceeds from crime with the help of cryptocurrency, which need to be addressed in the investigation process, are described. Namely, the main groups of criteria that indicate the use of virtual currencies in such crimes are identified. Such factors are divided into two groups: general, which are used in many methods of investigating crimes in cyberspace, and indicators that indicate the criminal activity of virtual currency providers.

In this study the investigative tools and methodologies of laundering of crime proceeds using virtual currencies, features that indicate that the suspect used virtual assets in criminal activities are considered. Particular attention is paid to data related to software associated with the use of virtual currencies and browsing history containing virtual currency related websites, as well as evidence that can be obtained during the investigation of a suspect's computer or mobile device.

The circumstances to be established in the course of the investigation of laundering of crime proceeds using virtual currencies and the evidence confirming such circumstances are highlighted.

Key words: investigation, laundering of crime proceeds, virtual currencies, cryptocurrency, virtual currency providers.

Постановка проблеми. Безсумнівно, сучасні технології створюють нові можливості не лише в повсякденному житті, а й в протиправних діях. Так наприклад, нині дедалі більш поширеним стає використання криптовалюти в процесі відмивання злочинних коштів. Оскільки криптовалюта є відмінним платіжним засобом, що дозволяє приховувати джерело доходу, її використання в злочинній діяльності становить серйозні труднощі для правоохоронних органів під час розслідування легалізації (відмивання) доходів, отриманих злочинним шляхом.

Стан опрацювання. Роль криптовалюти в злочинах, пов'язаних із легалізацією (відмиванням) доходів, отриманих злочинним шляхом, досліджувалася в тому чи іншому аспекті багатьма науковцями, зокрема такими як В. Білинський, В. Динту, О. Дикий, О. Карапетян, А. Мітрофанов.

Що стосується розслідування легалізації доходів, отриманих злочинним шляхом із використанням віртуальних валют, із точки зору практичної діяльності працівників слідчих органів, необхідно підкреслити актуальність цієї теми та необхідність здійснення подальших досліджень у цій сфері.

Мета статті полягає в з'ясуванні особливостей методики розслідування легалізації (відмивання) злочинних коштів із використанням криптовалюти, а також дослідженні правового статусу віртуальних активів в Україні.

Виклад основного матеріалу. Міжнародна спільнота, розуміючи весь масштаб нових викликів, пов'язаних із віртуальними активами, прийняла відповідні нормативні акти, щоб забезпечити належне регулювання нових відносин та попередити злочинне використання таких фінансових інструментів.

Так, 21 червня 2019 року Група з розробки фінансових заходів боротьби з відмиванням грошей (FATF) опублікувала Керівництво з ризик-орієнтованого підходу до віртуальних активів та постачальників послуг із переказу віртуальних активів [1]. Одночасно FATF прийняла Пояснювальну записку до Рекомендації 15 «Нові технології», яка встановлює додаткові вимоги для віртуальних активів і провайдерів послуг у сфері віртуальних активів. Нові вимоги FATF поширюють сферу дії регулювання з протидії відмиванню грошей і фінансуванню тероризму на операції з обміну віртуальними активами і на широке коло провайдерів послуг і продуктів у криптосфері, включаючи зберігачів і біржі. Цей документ призначений для сприяння виконавчим органам країн у розумінні сутності віртуальних активів, а також допомоги у виробленні регулятивних і наглядових заходів щодо діяльності, пов'язаної з віртуальними активами, провайдерами послуг у сфері віртуальних валют [1].

Україна з метою імплементації цих міжнародних стандартів, водночас адаптуючи їх до національних обставин, прийняла відповідні зміни в законодавстві, фактично легалізуючи віртуальні валюти. Так, 28 квітня 2020 року набув чинності Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», в якому вперше на рівні національного законодавства вводиться поняття «віртуальні активи» та визначається «суб'єкт державного фінансового моніторингу в цій сфері – Міністерство цифрової трансформації України» [2].

Крім того, що цей Закон легалізує віртуальні активи, створює основу для їх існування та визнання Україною, також встановлюється «обов'язок постачальників послуг, пов'язаних з обігом віртуальних активів, здійснювати верифікацію клієнтів, крім випадків, якщо сума проведення фінансової операції з віртуальними активами не перевищує 30 тисяч гривень» [2]. Також зазначений нормативно-правовий акт виводить із тіні операції, пов'язані з віртуальними валютами, що своєю чергою є превентивними заходами в боротьбі з легалізацією злочинних коштів за допомогою віртуальних валют, та сприяє органам досудового розслідування в розслідуванні таких злочинів, адже дає змогу на початкових етапах зібрати якнайбільше доказової інформації.

Незважаючи на це, деталізація правового регулювання ринку віртуальних активів нині відсутня. Нині у Верховній Раді України перебуває на розгляді проєкт Закону України «Про віртуальні активи» № 3637 [3]. Передбачається, що такий нормативно-правовий акт детально врегульовуватиме поняття та правовий статус віртуального активу, а також питання прав власності та здійснення правочинів із такими активами в Україні.

Таким чином, можна підсумувати, що в Україні лише починає формуватися нормативна основа правового регулювання обігу віртуальних валют. Проте наша держава знаходиться на вірному шляху та поступово впроваджує норми права в цій сфері, що рекомендовані міжнародною спільнотою.

Незважаючи на це, сучасний світ не стоїть на місці і не чекає, поки з'явиться правове регулювання тієї чи іншої сфери, навпаки, недосконаліть нормативного регламентування ринку віртуальних активів злочинці використовують на власну користь, під час незаконної діяльності, в тому числі в процесі легалізації коштів, здобутих злочинним шляхом. А тому слідча практика має пристосовуватися до таких реалій, формувати нові методичні положення та рекомендації розслідування легалізації злочинних коштів із використанням віртуальних активів.

Легкість легалізації коштів, отриманих злочинним шляхом за допомогою криптовалюти, зумовлює популярність такого платіжного засобу у злочинних колах. На думку О. Карапетян та В. Білинського, «відсутність зв'язку між рахунками у віртуальних валютах і реальними людьми в поєднанні з можливістю володіти необмеженою кількістю рахунків зумовлює сприятливе середовище для створення нових складних моделей, спрямованих на приховування незаконного походження коштів» [4, с. 116].

Тому, на нашу думку, важливість норм Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», що стосуються необхідності верифікації користувачів віртуальних валют, для слідчої практики важко переоцінити.

Одним із перших прикладів використання віртуальної валюти в процесі відмивання злочинних доходів можна назвати компанію Liberty Reserve, засновану в Коста-Ріці А. Будовським, яка працювала «як банк чорного ринку – кримінальний бізнес, що допомагав злочинцям здійснювати незаконні угоди». За сім років Liberty Reserve проведено 55 млн незаконних угод та легалізовано $6 млрд. Компанія свідомо приймала підозрілі депозити, конвертуючи їх у власну цифрову валюту (LR), після чого знову здійснювалася конвертація в чисту валюту після процедури позбавлення коштів будь-яких ознак місця їхнього походження [5, с. 79]. Пройшовши формальну реєстрацію, клієнт переводив справжні кошти у фірми-обмінники третіх країн, в подальшому валюта конвертувалася в LR, після чого надходила на рахунки Liberty Reserve. Звідти вже на віртуальну валюту можна було придбати наркотики, номери викрадених кредитних карток чи інші речі, перевівши потрібну суму LR на рахунок продавця, відкритий також у LR. Непотрібні LR конвертувалися в реальну валюту через ті самі обмінники. Діяльність із відмивання грошей проводилась цілком анонімно. Ця схема була виявлена Службою фінансових розслідувань США [6].

Слід також зазначити, що Управлінням ООН із наркотиків та злочинності (UNODS) в рамках проєкту «Посилення співпраці країн-членів GUAM (Грузія, Україна, Азербайджан та Молдова) на національному та регіональному рівнях у боротьбі з відмиванням коштів, а також у процесі вилучення та конфіскації доходів, отриманих злочинним шляхом» розроблено посібник «Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies» [7]. Метою цього посібника є надання практичної допомоги слідчим та прокурорам у процесі виявлення, розслідування, доказування та вилучення доходів, отриманих злочинним шляхом, легалізованих за допомогою віртуальних валют.

Так, у вказаному дослідженні автори, аналізуючи особливості фінансових інструментів, за допомогою яких відбувається легалізація, надають власні методичні рекомендації щодо розслідування та доказування легалізації злочинних коштів із використанням криптовалюти.

Розглядаючи практичні аспекти виявлення таких злочинів, необхідно дослідити індикатори (фактори), які вказують, що відбулася легалізація злочинних коштів за допомогою віртуальних валют. UNODS виділяє дві групи індикаторів таких злочинів.

«До першої належать наступні:

1) невідповідність між даними, що ідентифікують клієнта, та IP-адресою.

Наприклад, якщо користувач надає інформацію для створення облікового запису із зазначенням адреси у Великобританії, тоді як всі IP-адреси, пов'язані з діяльністю замовника, визначаються як такі, що знаходяться в Японії;

2) підозрілі IP-адреси та підозрілі імена користувачів (прізвиська, псевдоніми, номери ICQ) також можуть свідчити про злочинні грошові потоки;

3) спроби входу з ненадійної IP-адреси або з IP-адреси користувача, раніше визначеної як така, що пов'язана з підозрілою діяльністю» [7].

Ці індикатори є загальними та застосовуються в багатьох методиках розслідування злочинів у кіберпросторі. Тому автори окремо наводять фактори, що вказують на «злочинну діяльність саме провайдерів віртуальних валют:

1) велика кількість банківських рахунків, що знаходяться в одного провайдера віртуальної валюти або компанії з обміну віртуальних валют (можуть знаходитися в різних країнах), очевидно, використовується як поточний рахунок (свідчить про розшарування діяльності), без явної ділової мети такої структури;

2) адміністратор віртуальної валюти або компанія з обміну віртуальних валют, розташована в одній країні, але рахунки відкриті в інших країнах, де вона не має значної клієнтської бази (відсутнє обґрунтування такої діяльності);

3) переміщення коштів між банківськими рахунками, які ведуться різними адміністраторами віртуальної валюти або компаніями, що здійснюють обмін віртуальними валютами, розташованими в різних країнах (може свідчити про розшарування діяльності, бо вона не відповідає типовій бізнес-моделі);

4) обсяг та частота операцій із готівкою (іноді нижче порогової звітності), що проводяться власником провайдера віртуальної валюти або компанії з обміну віртуальними валютами, без економічної вигоди та змісту» [7].

Як відомо, легалізація злочинних коштів може здійснюватися різними способами, злочинці вигадують найрізноманітніші схеми відмивання коштів. Тому, на нашу думку, варто звернути увагу саме на особливості, які свідчать, що підозрюваний використовував у злочинній діяльності віртуальні валюти. Надалі це значно спростить процес розслідування легалізації доходів, отриманих злочинним шляхом, адже слідчий чітко розумітиме, з яким фінансовим інструментом він має справу, як розшукати докази і яким чином працювати з такими доказами.

Деякі віртуальні валюти, особливо децентралізовані, передбачають встановлення спеціального програмного забезпечення. Наявність такого програмного забезпечення на досліджуваному комп'ютері також може свідчити про використання віртуальних валют у злочинній діяльності.

Наведемо приклади програмного забезпечення, що необхідне для використання найвідомішої віртуальної валюти – Bitcoin. Програмне забезпечення, встановлене на комп'ютері для використання мережі Bitcoin, називається біткойн-гаманцем. У мережі доступна безліч різноманітних програмних пакетів біткойн-гаманців, наприклад, BitcoinCore, MultiBit, Hive, BitcoinArmory, Electrum. Деякі з цих програмних пакетів після встановлення завантажують повну копію всього блокчейну Bitcoin. Слід звернути увагу, що це дуже великий розмір – майже 20 гігабайтів. Розуміння слідчим зазначених фактів може бути корисним для ідентифікації каталогу даних, що використовується програмним забезпеченням Bitcoin. Крім того, наявність файлу гаманця, який часто називають «wallet.dat», також свідчить про використання мережі Bitcoin [7].

Слід взяти до уваги, що не всі віртуальні валюти передбачають необхідність встановлення спеціального програмного забезпечення. Наприклад, клієнт Ripple працює як додаток JavaScript у браузері користувача. Деякі віртуальні валюти пропонують або завантажити програмне забезпечення, або здійснювати взаємодію через браузер як варіант використання віртуальної валюти. Крім того, торгівля віртуальними валютами на біржах віртуальних валют, як правило, здійснюється у браузері. Таким чином, закладки, історія перегляду та кеш-пам'ять комп'ютера підозрюваного також потребують ретельного дослідження, а отримані докази можуть надати цінні відомості з приводу використання віртуальних валют [7].

Крім того, програмне забезпечення для віртуальних валют та дані з історії перегляду, що пов'язані з використанням віртуальних валют, також можна знайти на мобільних пристроях. Тому матеріали, зібрані в результаті дослідження мобільних пристроїв, можуть містити важливу інформацію для доказування фактів використання віртуальних валют для відмивання доходів, отриманих злочинним шляхом [7].

Як і в багатьох випадках, пов'язаних із розслідуванням злочинів у кіберпросторі, комп'ютер підозрюваного є цінним джерелом доказів. Звичайно, таке твердження не обмежується лише комп'ютером як річчю, а також стосується будь-яких інших носіїв інформації (компакт-диски, зовнішні жорсткі диски, флеш-накопичувачі тощо), які знайдені разом із комп'ютером підозрюваного або про які відомо, що використовувалися під час роботи з ним.

Так, автори посібника «Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies» виділяють такі категорії доказів, які можна отримати з комп'ютера підозрюваного:

1) докази у вигляді облікових даних, історії відвідувань вебсайтів, електронних листів тощо, які дають змогу встановити взаємодію підозрюваного з провайдером віртуальної валюти або біржою віртуальних валют;

2) докази, які доводять наявність у підозрюваного певної вартості віртуальної валюти;

3) IP-адреса комп'ютера в певний час може бути пов'язана з відомими підозрілими операціями чи іншою фінансовою діяльністю;

4) докази використання послуг віддаленого зберігання, де може зберігатися вираження вартості віртуальної валюти;

5) паролі та інші облікові дані, які можуть бути використані в процесі розслідування [7].

Отже, під час розслідування легалізації (відмивання) коштів, здобутих незаконним шляхом, яка здійснюється з використанням криптовалюти, необхідно враховувати специфіку віртуальних валют, особливості їх функціонування та обігу, технічні та інформаційні характеристики кіберпростору, в якому здійснюється обмін такими активами. На практиці слідчому для належного розслідування та доведення фактів легалізації злочинних коштів слід враховувати особливості, які вказують на використання в процесі такого злочину віртуальних валют. Індикатори, що свідчать про використання криптовалюти в такій злочинній діяльності, умовно можна поділити на дві групи: загальні фактори, які свідчать, що легалізація злочинних доходів відбулася з використанням технологій глобальної мережі, та дані, що вказують на злочинну діяльність провайдерів віртуальних валют. Також варто зазначити, що найбільшу кількість інформації слідчий під час розслідування отримує за допомогою електронних доказів, саме вони найчастіше використовуються в процесі доказування.

ЛІТЕРАТУРА

1. Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF. Paris, 2019. URL: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html (дата звернення 11.10.2020).

2. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 06.12.2019 р. № 361-IX. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text (дата звернення 11.10.2020).

3. Про віртуальні активи : проєкт Закону № 3637 від 11.06.2020 р. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110 (дата звернення 11.10.2020).

4. Карапетян О., Білинський В. Злочинні технології збагачення з використанням криптовалют та особливості їх розслідування. *Актуальні проблеми правознавства.* 2018. № 2 (14). С. 115–120.
5. Dyntu V., Dykyi O. Crypto currency in the system of money laundering. *BalticJournal of Economic Studies*, 2018. № 5. С. 75–81.
6. Власти США закрыли крупнейшую независимую электронную платёжную систему Liberty Reserve. URL: https://ru.wikinews.org/wiki/Власти_США_закрыли_крупнейшую_независимую_электронную_платёжную_систему_Liberty_Reserve (дата звернення 11.10.2020).
7. Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies. *United Nations Office on Drugs and Crime*, 2014. URL: https://www.imolin.org/pdf/UNODC_VirtualCurrencies_final_EN_Print.pdf (дата звернення 11.10.2020).