УДК 343.98
DOI https://doi.org/10.32782/2524-0374/2023-4/139

МОЖЛИВОСТІ ЦИФРОВОЇ КРИМІНАЛІСТИКИ ПІД ЧАС РОЗСЛІДУВАННЯ ЛЕГАЛІЗАЦІЇ КОРУПЦІЙНИХ ДОХОДІВ

POSSIBILITIES OF DIGITAL FORENSICS DURING THE INVESTIGATION OF LEGALIZATION OF CORRUPTION INCOME

Латиш К.В., к.ю.н., доцентка,
асистентка кафедри криміналістики
Національний юридичний університет імені Ярослава Мудрого

Демидова Є.Є., к.ю.н., доцентка,
доцентка кафедри криміналістики
Національний юридичний університет імені Ярослава Мудрого

Капустіна М.В., к.ю.н., доцентка,
доцентка кафедри криміналістики
Національний юридичний університет імені Ярослава Мудрого

У статті аналізуються можливості цифрової криміналістики під час розслідування легалізації корупційних доходів у двох вимірах. З одного боку, здійснюється дослідження інструментів цифрової криміналістики, за допомогою яких можна ідентифікувати, зібрати та дослідити такі дії. З іншого боку, простежується перелік цифрових інструментів, які використовуються для вчинення легалізації корупційних доходів у цифровій площині з використанням віртуальних активів. Цифрові технології, які кожного дня з'являються, видозмінюються, трансформуються, використовуються не лише з правомірною метою, але й злочинною. Разом з тим, разючою відмінністю використання саме цифрових технологій з метою легалізації корупційних доходів, є те, що ті цифрові сліди, що залишаються, майже неможливо знищити, змінити чи модифікувати. Тому можливостей для ідентифікації способу правопорушення та особи, яка його вчинила, стає більше, про які навіть не завжди знає і сама особа, зокрема через брак знань у цифровій площині. Віртуальні активи – це відносно нова категорія для правоохоронної системи, оволодіння пошук та фіксації яких потребують технологічної модернізації оснащення та знань працівників відповідно до сучасних тенденцій. На цей час відсутні комплексні розробки щодо можливостей виявлення та фіксації віртуальних активів та цифрових слідів з метою подальшого набуття ними статусу доказів у відповідному процесі. Такою неврегульованістю та відсутністю напрацьованої практики документування і користуються особи, які вдаються до таких дій. З цих причин і почала формуватися цифрова криміналістика в якості окремого напрямку, який поєднує в собі положення юридичних наук та технічних наук. Саме синергія цих двох наук, об'єднання наукових та практичних знань, дадуть поштовх формуванню ефективної практики розслідування різних кримінальних правопорушень. Ця практика знаходиться на первинному щаблі свого формування, наростаючі «крок за кроком» з плином часу та дослідженням появи нових цифрових інструментів. Тому лише окремі можливості використання цифрової криміналістики під час розслідування легалізації корупційних доходів і розглянемо у цій статті.

Ключові слова: цифрова криміналістика, легалізація корупційних доходів, OSINT, інструменти цифрової криміналістики.

The article analyses the possibilities of digital forensics in investigating money laundering in two dimensions. On the one hand, digital forensics tools can be used to identify, collect evidence and investigate such crimes. On the other hand, the list of digital tools used to commit money laundering in the digital domain using virtual assets is analyzed. Digital technologies, which appear, change and transform daily, are used for legitimate and criminal purposes. At the same time, a striking difference in the use of digital technologies for the purpose of money laundering is that the digital traces that remain are almost impossible to destroy, change or modify. Therefore, there are more opportunities to identify the method of the offence and the person who committed it, which are not even always known to the person, in particular, due to a lack of knowledge in the digital domain. Virtual assets are a relatively new category for the law enforcement system, and mastering the search and recording of them requires technological upgrades to the equipment and knowledge of employees in line with current trends. At present, there are no comprehensive developments on the possibility of further detecting and recording virtual assets and digital traces to acquire the status of evidence in the relevant process. People who resort to such actions use this lack of regulation and the absence of established documentation practices. For these reasons, digital forensics has emerged as a separate field combining the provisions of law and engineering. The synergy of these two sciences, combining scientific and practical knowledge, will give impetus to developing effective practices investigating various criminal offences. This practice is at the initial stage of its formation, growing "step by step" over time and by researching the emergence of new digital tools. Therefore, this article will consider only some possibilities of using digital forensics to investigate money laundering.

Key words: digital forensics, legalization of corruption proceeds, OSINT, digital forensics tools.

Технологізація способів легалізації корупційних доходів пришвидшується з кожним днем. Разом з тим, специфіка таких змін містить «дві сторони медалі», адже такі технології можуть давати можливість не лише маскувати вчинення легалізації корупційних доходів, але й «оголяти» у цифровому просторі можливості їхньої ідентифікації та подальшої протидії. Така ідентифікація може бути здійснена з огляду на ті цифрові сліди, які залишаються у мережі. Саме тому особливої актуальності набувають розробки цифрової криміналістики, яка ще більше підсилила «технологізацію» традиційної криміналістики, розроблення та впровадження інформаційних, цифрових, телекомунікаційних та інших технологій [1, с. 12], а також наявні тенденції практичної спрямованості криміналістичних розробок та інноваційних продуктів, їхнього прагматичного орієнтування [2, с. 22].

Про актуальність проблематики свідчить і наявна кількість наукових досліджень у цій сфері, зокрема це праці А. А. Музики, А. В. Наумова, В. А. Світличного, В. М. Шевчука, В. Ю. Шепітька, М. В. Шепітька та інших.

Деякі науковці відносять цифрову криміналістику до нової галузі криміналістичних знань або певного стратегічного напряму, яка визначає роль цифрових доказів у процесі доказування [1, с. 16]. Інші науковці зазначають, що цифрова криміналістика є «однією з галузей криміналістики, яка зосереджена на кримінально-процесуальному праві і доказах стосовно комп'ютерів і пов'язаних з ними пристроїв» [3, с. 379]. Однак, слід відрізняти цифрову криміналістику від суміжних галузей: розслідування інцидентів інформаційної безпеки в організаціях, банківських установах, у яких дослідження комп'ютерного устаткування має важливе значення [4, с. 121]. Інструменти циф-

рової криміналістики мають доволі істотне значення для процесу розслідування, оскільки сприяють розслідуванню та дозволяють підійти до цього процесу з неочікуваної для особи, яка вчиняє кримінальне правопорушення, сторони. Оскільки вона, плануючи свою злочинну діяльність, не передбачає можливості використання інструментів цифрової криміналістики зі сторони досудового розслідування, а тому не буде намагатися приховувати свої сліди у цифровому просторі.

На відміну від «класичного» відмивання корупційних доходів, що були отримані злочинним шляхом, за допомогою використання банківської системи, кіберлегалізація доходів, заснована на використанні різних типів транзакцій: від банківських переказів, поповнення або зняття готівки до використання цифрової валюти. Розкриття та відстеження злочинних фінансових ланцюгів у цьому випадку є складним завданням для правоохоронних органів, оскільки заплутані схеми є справжнім викликом, а для цього потрібні кваліфіковані спеціалісти у кібербезпеці, належне програмне та технічне забезпечення, що зможе якісно та ефективно протидіяти кіберлегалізації доходів [5, с. 106].

Ще одним підтвердженням таких негативних тенденцій використання віртуальних активів для можливої подальшої легалізації коруційних злочинних доходів є те, що на кінець березня 2021 року українські державні службовці задекларували 46,351 біткоїнів, що складає близько $1.7 мільярда [6]. Використання віртуальних активів у звичайному обігу не є характерним для української грошової системи, тим паче для державних службовців, які заробітну платню отримують у національній валюті – гривні. Рівень використання криптовалюти у злочинній сфері в Україні є значним та за міжнародними оцінками (The Chainalysis 2021 Crypto Crime Report [7]) посідає третє місця за обсягом транзакцій на електронні гаманці, асоційовані з інтернет-магазинами наркотиків, які функціонують у darknet. Загальний обсяг транзакцій з України на гаманці інтернет-магазинів та з гаманців інтернет магазинів на Україну склав у 2020 році близько $100 млн. [6]. У цьому контексті є цікавою така ситуація, коли під час виконання повноважень голова однієї з обласних державних адміністрацій задекларував криптовалюту Bitcoin вартістю 13,1 млн. грн. Криптовалюта Bitcoin має публічну адресу (Public Address), яка є відкритою та підтверджує належність певній особі. Голова не зміг надати публічну адресу криптовалюти. Водночас, за даними податкової загальний дохід цієї особи та членів його сім'ї з 2001 по 2020 рік складав менше 1 млн грн (загалом 880 682,56 грн) [8].

Традиційною технологією відмивання коштів в цій сфері є придбання за «злочинні» кошти різних видів віртуальних активів (криптовалют) та на наступному етапі за допомогою різних бірж та спеціальних сервісів-міксерів подрібнити початкові монети та конвертувати їх в інші криптовалюти [9, с. 82]. Однак, все ж таки є можливість для відновлення історії переходів конкретного віртуального активу (криптовалюти), і на відміну від звичайних баз даних, змінити або видалити історію цих записів не можливо, можна додати тільки нові. Навіть, у випадку, якщо віртуальний актив придбається за готівкові кошти через посередництво третьої особи (посередника), у будь-якому разі відбувається відображення трансакцій в розподіленому реєстрі на користь особи, що користується послугами посередника, зокрема, створення гаманця, який містить публічну адресу криптовалюти, придбання криптовалюти. У блокчейні (ланцюжку блоків) як розподіленому реєстрі усі трансакції записуються в незмінних блоках. Блокчейн грає роль історичного реєстру всіх записів – від першого до останнього блоку та існує лише в електронному вигляді. У блокчейні (розподіленому реєстрі) за певний період часу відбувається кілька трансакцій, як наслідок, записи про трансакції включається в один блок, який є базовим елементом структури блокчейну. Він складається з двох частин – заголовка (Head) і корисного навантаження (Payload) – власне запису здійснених трансакцій. Як було зазначено вище, будь-яка криптовалюта, що належить тій чи іншій особі характеризується наявністю публічної адреси. За визначенням, публічна адреса (Public Address) – це криптографічний хеш відкритого ключа, який є унікальним набором символів, що складається з букв і цифр. Публічна адреса біткоїна (Bitkoin) включає у себе від 26 до 35 символів. При цьому публічна адреса дозволяє дізнатися всю історію трансакцій конкретного суб'єкта, а саме: дату набуття криптовалюти, наявність криптовалюти на певну дату, кількість криптовалюти, якою володіє особа [10].

Таким чином, необхідним є встановлення такого електронного гаманця з криптовалютою, встановлення його приналежності конкретній особі, визначення часу та способу яким ця цифрова валюта потрапила до гаманця (надати цьому правову оцінку) і перевірити чи мала ця особа легальні фінансові джерела доходу для такого придбання. Проте є складнощі з ідентифікацією номера гаманця, адже немає обов'язку державному службовцю десь цю інформацію вказувати, однак, для цього можна використати традиційні процесуальні важелі, встановлені чинним законодавством (наприклад, отримати дозвіл суду на такі дії).

Як зазначає М.В. Карчевський вплив віртуальних активів на протидію корупції слід розглядати у трьох вимірах:

1) новий вид неправомірної вигоди;

2) нові можливості протидії злочинності;

3) антикорупційний потенціал технологій розподіленого зберігання даних [6].

Деякі автори виділяють такі основні інструменти відмивання корупційних доходів:

– фіктивні послуги;

– використання афілійованих осіб для надання псевдопослуг;

– передплата за товари і послуги підконтрольним особам з подальшою непоставкою/невиконанням;

– заниження вартості товарів державною компанією при реалізації компаніям-посередниками для акамулювання прибутків;

– укладання завідомо неправомірних угод по придбанню продукції за цінами, встановленими для соціальних потреб, з подальшою її реалізацією;

– використання підприємств з ознаками фіктивності;

– «торгівля» державними послугами з видачі/оформлення дозвільних документів;

– використання банківських рахунків, відкритих за межами України;

– відхилення конкурентних заяв на участь в тендерах на користь підконтрольних компаній, що пропонують значно вищі ціни [11].

Способи і методи, які використовують злочинці у процесі відмивання корупційних доходів, отриманих у сфері кіберзлочинності, є досить різноманітними:

− використання чужих рахунків, реквізити яких були викрадені або втрачені;

− залучення «дропів» – це особи, які є безпосередніми помічниками у вчиненні злочину, у такий спосіб як зняття готівки з різних банкоматів, оскільки готівкові кошти майже неможливо відслідкувати (поза межами платіжних, банківських систем) або переказ коштів між рахунками, що дозволяє заплутати ланцюг переказів, і в такий спосіб залишитися непокараним;

− якщо в традиційну платіжну систему інтегровані онлайн-платежі або інші онлайн-послуги, то гроші можуть бути швидко переведені в електронні, а згодом їх можна практично анонімно перевести на рахунки іноземної держави;

− купівля електронних грошей, криптовалюти;

– використання доходів, отриманих за допомогою кіберзлочинів, шляхом придбання різноманітних товарів або послуг для подальшого їх збуту й отримання готівки (оплата послуг у мережі Інтернет, товарів в інтернет-магазинах, надання або повернення фінансових позик, купівля комп'ютерних ігор, програмного забезпечення тощо) [5, с. 108–109];

– технології розподіленого зберігання даних (BlockChain). Поява технологій розподіленого зберігання даних (BlockChain) та заснованих на таких технологіях криптовалютних платіжних систем істотно змінює процес протидії злочинності. З одного боку, криптовалюти стали новим інструментом злочинців. З іншого – наявність у відкритому доступі всієї бази даних транзакцій у системі криптовалюти дає правоохоронцям принципово нові інструменти боротьби зі злочинністю [6];

– залучення осіб, які не мають з «корупціонером» близьких родинних зв'язків, в той же час пов'язані іншими зв'язками (далекі родичі, водії, помічники);

– зарахування коштів в якості авторської винагороди;

– неоднарозове отримання спадщини від осіб, не пов'язаних родинними зв'язками;

– придбання власності за кордоном;

– придбання корпоративних прав, надання фінансової допомоги або збільшення статутного капіталу підприємствам, власниками яких є особи афілійовані із посадовими особами державних підприємств, установ, організацій;

– погашення кредитів, які були використані для придбання елітного житла, автомобілів VIP-класу, дорогоцінних металів та каміння, інших активів [11, с. 40].

У структурі правоохоронних органів є Департамент кіберполіції, який володіє технологіями виявлення криптогаманців, у тому числі із використанням даних з відкритим кодом (OSINT). Необхідно звернути увагу на істотну роль прибуткових та неприбуткових організацій у цьому процесі, а також важливості співпраці з такими установами. Так, кіберполіція підписала меморандум та стала партнером проєкту з виявлення криптогаманців у рамках ініціативи Scamfari, метою якого є встановлення адрес криптогаманців, на які збирають «донати» для підтримки військової агресії рф проти України [12]. Результати якого вже дали певні плоди [13] та технологічні напрацювання якого можуть безсумнівно використовуватися і в інших видів кримінальних правопорушень, у тому числі для виявлення легалізації корупційних доходів.

Крім того, важливо зауважити, що важливою є співпраця з криптовалютними біржами світу щодо обміну інформацією, яка може використовуватися під час виявлення та розшуку активів. Так, Національне агентство з питань виявлення, розшуку та управління активами (АРМА) встановило таку співпрацю з 5 великими криптобіржами, що дозволяє: 1) встановлювати факти існування цифрових і віртуальних активів в учасників кримінального провадження; 2) отримання ідентифікаційних даних власника криптовалютного гаманця (інформації або навіть документу про проведення операції, номери рахунків, на які виводяться кошти) [14].

Таким чином, цифрова криміналістика має значний потенціал у боротьбі з легалізацією корупційних доходів. Вона дозволяє виявляти, збирати та аналізувати цифрові сліди (інформацію про транзакції, що відбувалися в онлайн середовищі, встановлювати зв'язки між різними цифровими даними, з'ясувати, що певні операції були виконані з конкретного комп'ютера або мобільного пристрою тощо). Однак, для успішного розслідування необхідна співпраця між різними правоохоронними органами та особами, що володіють спеціальними знаннями у цій сфері.

ЛІТЕРАТУРА

1. Шепітько В., Шепітько М. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. *Право України.* № 8. С. 12–27.
2. Шевчук В. М. Криміналістична інноватика: поняття, функції, завдання та перспективи досліджень. *Теорія та практика судової експертизи і криміналістики.* 2020. Вип. 22. С. 20–40. DOI: 10.32353/khrife.2.2020.01 (дата звернення: 12.04.2023).
3. Колодіна А.С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Юридичний науковий електронний журнал*. 2022. № 4. С. 378-380. http://lsej.org.ua/4_2022/90.pdf (дата звернення: 20.04.2023).
4. Гриців О. Криміналістика в комп'ютерних системах: процеси, готові рішення. *Вісник Національного університету «Львівська політехніка». Автоматика, вимірювання та керування.* 2013. № 774. С. 120–126.
5. Думчиков М. О., Бондаренко О. С. Кримінологічні аспекти протидії легалізації корупційних доходів в кіберпросторі. *Правові горизонти.* 2021. № 14 (2). С. 105–110.
6. Карчевський М. В. Протидія корупції: інновації та імітації. URL: https://karchevskiy.org/2021/11/18/протидія-корупції-інновації-та-іміта/ (дата звернення: 20.04.2023).
7. Grauer K., Updegrave H. The Chainalysis 2021 Crypto Crime Report. URL: https://go.chainalysis.com/2021-Crypto-Crime-Report.html (дата звернення: 20.04.2023).
8. Керівник ДРС не зміг підтвердити володіння біткоїнами вартістю 13 млн грн. *Національне Агентство з питань запобігання корупції.* URL: https://nazk.gov.ua/uk/novyny/deklaruvannya/kerivnyk-drs-ne-zmig-pidtverdyty-volodinnya-bitkoyinamy-vartistyu-13-mln-grn-golova-nazk-vymagaye-prytyagnuty-jogo-do-dystsyplinarnoyi-vidpovidalnosti/ (дата звернення: 20.04.2023).
9. Актуальні методи, способи, інструменти легалізації (відмивання) злочинних доходів та фінансування тероризму (сепаратизму). Київ, 2021. URL: https://fiu.gov.ua/assets/userfiles/200/Typologies%20of%20the%20SFMS/UKR_Typology_2021_26_05.pdf (дата звернення: 20.04.2023).
10. Довідка № 199/21 про результати проведення повної перевірки декларації […], складеної НАЗК. *Національне Агентство з питань запобігання корупції.* URL: https://nazk.gov.ua/wp-content/uploads/2021/07/Kucher_2020_na-sajt.pdf (дата звернення: 20.04.2023).
11. Типологічні дослідження Державної служби фінансового моніторингу України за 2016, 2015, 2014 роки. Київ, 2017. 126 с.
12. Кіберполіція викрила зловмисників у фінансуванні окупантів. *Офіційний веб портал Національної поліції України.* URL: https://cyberpolice.gov.ua/news/kiberpolicziya-stala-partnerom-proyektu-z-vyyavlennya-kryptogamancziv-povyazanyx-iz-terorystychnoyu-ta-pidsankczijnoyu-diyalnistyu-6808/ (дата звернення: 20.04.2023).
13. Кіберполіція викрила зломвисників у фінансуванні окупантів. *Офіційний веб портал Національної поліції України.* URL: https://www.npu.gov.ua/news/kiberpolitsiia-vykryla-zlovmysnykiv-u-finansuvanni-okupantiv (дата звернення: 20.04.2023).
14. АРМА налагодило співпрацю з п'ятьма найбільшими криптобіржами світу. *Мультимедійна платформа іномовлення України «Укрінформ».* URL: https://www.ukrinform.ua/rubric-economy/3615124-arma-nalagodilo-spivpracu-z-patma-najbilsimi-kriptobirzami-svitu.html (дата звернення: 20.04.2023).