УДК 343.9
DOI 10.33244/2617-4154.1(8).2022.192-199

Д. З. Чайковський,
Державний податковий університет
e-mail: chaykovskiy97@gmail.com
ORCID ID 0000-0002-5779-8290

КРИМІНОЛОГІЧНІ АСПЕКТИ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ, ПОВ'ЯЗАНОЇ З ВИКОРИСТАННЯМ БЕЗГОТІВКОВИХ АКТИВІВ (КРИПТОВАЛЮТИ)

XXI століття характеризується стрімким розвитком сучасних інформаційних технологій, які щодня стають досконалішими, а обсяг обробки даних – усе більшим. Інформаційні ресурси наразі становлять не тільки дані на кошти, а саме електронні валюти та безготівкові ресурси, які курсують з одного електронного гаманця до іншого.

Використання електронних валют у злочинній сфері є досить актуальним та поширеним явищем, оскільки це дає можливість анонімно фінансувати та отримувати дохід із зайняття злочинною діяльність, оскільки криптовалюта за своєю природою наділена певною конфіденційністю та не несе майже ніякої інформації про її власника.

У ході дослідження використано інформаційно-аналітичний, формально-юридичний, порівняльний та індуктивний методи.

Основними результатами дослідження є висвітлення власного теоретичного підходу щодо запобігання злочинності, пов'язаної з використанням безготівкових активів (криптовалюту), покращити вже існуючі методи запобігання цього виду злочинності.

Обмеження з боку держави доволі сильно вплинули на злочинний світ, особливо на наркотичний бізнес, тому що більшість операцій з купівлі та продажу наркотичних засобів і їх прекурсорів відбувається в електронній валюті. Звісно, система обмежень НБУ неідеальна, оскільки вона не регулює безпосереднє створення криптовалюти та її переміщення на персональні криптогаманці. Однак заборона купівлі та конвертації значно ускладнює злочинні процеси і на деякий час майже повністю зриває налагоджений злочинний конвеєр. Щоб ефективно запобігти цій сучасній формі злочинності варто більше приділяти уваги методам та способам попередження її розвитку. Наразі такими методами можуть бути моніторинг, контроль обігу, розширення міжнародної співпраці для відслідковування руху транзакцій.

Ключові слова: *безготівкові активи, блокчейн, електронна валюта, запобігання злочинності, протидія, криптовалюта, транскордонні валютні операції.*

Метою дослідження є визначення та дослідження кримінологічних аспектів запобігання злочинності, пов'язаної з використанням безготівкових активів (криптовалюти), а також висвітлення власного теоретичного бачення підходу щодо запобігання злочинам з використанням електронної валюти.

XXI століття варто характеризувати стрімким розвитком сучасних інформаційних технологій, які щодня стають більш досконалими, а обсяг обробки даних – усе більшим. Інформаційні ресурси наразі становлять не тільки дані на кошти, а саме електронні валюти та безготівкові ресурси, які курсують з одного електронного гаманця до іншого.

Аналіз останніх досліджень та публікацій. Кримінологічні засади злочинної діяльності з використанням криптовалют та технології блокчейн розглядали у своїх наукових працях: Р. І. Благута та А. В. Мовчан, М. В. Гребенюк та А. М. Черняк, Д. В. Казначеєва та А. О. Дорош, О. А. Клименко та М. В. Гуцалюк тощо. Проте це питання на сьогодні не є повністю дослідженим.

Виклад основного матеріалу. Криптовалюта (від англ. *Cryptocurrency*) – різновид цифрової валюти, емісія та облік якої виконується децентралізованою платіжною системою повністю в автоматичному режимі (без можливості внутрішнього або зовнішнього адміністрування). Принциповою особливістю криптовалют є збереження інформації у блокчейні, де асиметричне шифрування використовується для перевірки повноважень, а інші криптографічні методи – як доказ виконаної роботи та/або Proof-of stake [1]. Взагалі у використанні електронних валют немає нічого кримінально протиправного, навпаки, це великий прогрес у світі фінансової системи, прогрес в IT-технологіях. Нічого б небезпечного, якби не способи її отримання, видобутку та мети використання цих фінансових ресурсів. На сьогодні у світі існує значна кількість електронних валют, є як діючі, які користуються популярністю для інвестування, так і недіючі та непопулярні. Нас цікавить перша група.

Візьмемо до уваги найпопулярнішу електронну валюту – біткоїн, ціна якої за останні роки стрімко зросла. Цифрові гроші, зокрема біткоїн, подібні текстовим файлам. Відповідні транзакції відбуваються у форматі розсилки електронної пошти, тому для здійснення операції необхідно знати лише номер електронного гаманця. Отже, позитивними ознаками цієї валюти є: анонімність і швидкість транзакцій, суттєве спрощення фінансових операцій, відсутність єдиного власника, децентралізація тощо [2]. Сьогодні електронні валюти є зручним засобом розрахунку, валютного заробітку, способом фінансування для злочинців, які вчиняють правопорушення у різних сферах суспільного життя, наприклад у сфері наркобізнесу, тероризму та легалізації (відмиванні) коштів, які отриманні різними злочинними шляхами. Свою популярність електронні валюти отримали не тільки за те, що вони мають високу ринкову ціну, або те, що передача цих транзакцій швидка, а й за те, що власник залишається невідомим і тому злочинність у цій сфері, а саме з використанням криптовалюти, наділена природною латентністю.

Як відомо, що злочинність іде паралельно з технологічним процесом, і тому постають запитання: як протидіяти та як попереджати вчиненню кримінальних правопорушень у

певній сфері. Не поглиблюючись у злочинні схеми, які використовують електронну валюту як винагороду чи засіб вчинення кримінального правопорушення, візьмемо до уваги правопорушення, які вчиняються під час отримання криптовалюти, а це – викрадення електроенергії, самовільне під'єднання до енергетичних мереж, самовільне використання без засобів обліку, втручання в роботу електронних систем як державних, так і приватних, втручання в роботу обчислювальних систем. Наведені кримінальні правопорушення несуть загрозу насамперед енергетичній безпеці країни, оскільки для видобутку того самого біткоїну витрачається колосальний обсяг електроенергії. За останні роки спостерігаємо значну кількість новин від ЗМІ та пресцентрів органів правопорядку про те, як викрадається електроенергія для продуктивної роботи майнінг-ферм. Однак проблема в тому, що загроза полягає не тільки в економічній безпеці України, кримінальні правопорушення з використанням різних видів електронних валют несуть транснаціональну небезпеку, а саме можливість безслідно й анонімно фінансувати різни види кримінально протиправної діяльності з метою дестабілізації політичного та громадянського стану в будь-якій країні.

Якщо проаналізувати ряд країн, помітимо, що немає єдиного прикладу урегулювання обігу, добування, обміну та конвертації цих валют. На них не розповсюджується вплив державних органів у сфері регулювання обігу валют і цінних паперів. Привабливість криптовалют для злочинного світу пов'язана з тим, що в основі біткоїна та інших криптовалют лежить принцип децентралізації та система блокчейн (Blockchain): електронні гроші не мають прив'язки і не контролюються жодним фінансовим органом будь-якої країни, користувачі системи залишаються анонімними і мають рівні статуси. Основною перевагою виступає її анонімність, крім того, персональні дані власника електронного гаманця зберігаються в таємниці, і це лише набір символів, за якими неможливо вичислити власника, тому неможливо упізнати ім'я або адресу такого користувача, причому історія транзакцій є відкритою інформацією. Угоди, пов'язані з криптовалютою, теж анонімні, крім того, вони незворотні. Якщо свідчити про те, як держави ставляться до криптовалюти, то варто відмітити, що існують країни, які не схвалюють використання криптовалюти, до них належать Китай і Росія. У таких країнах, як Алжир, В'єтнам, Індонезія, Марокко, криптовалюта заборонена [3].

Небезпека використання цього виду валют полягає в тому, що вони не являють собою грошових знаків, грошових активів, а становлять хмарні активи, які можна використовувати як платіж. Варто зазначити, що, за результатами статистичного дослідження глобальної сервісної IT-компанії Triple-A, Україна входить у топ-10 країн за кількістю власників криптовалют, а це означає, що концентрація активів, які можна конвертувати для певної потреби, досить велика. До прикладу, весь обіг наркотичних засобів та прекурсорів в Україні здійснюється через електронні гаманці, оплачується національної валютою та згодом конвертується в будь-яку криптовалюту, а отже, відслідкувати рух активу можливо, а особу, яка здійснює трансакцію, ідентифікувати неможливо. Ще одна складність – це те, що купівля і продаж різних заборонених до обігу чи обмежених в обігу речовин здійснюється в системі даркнету. Даркнет (від англ. dark net) – оверлейна мережа, доступ до якої можливий лише через певне

програмне забезпечення, налаштування чи авторизацію, часто з використанням нестандартних комунікаційних протоколів та портів. Анонімна мережа являє собою систему не пов'язаних між собою віртуальних тунелів, що дозволяє передавати дані в зашифрованому вигляді. Даркнет відрізняється від інших розподілених однорангових мереж тим, що файлообмін відбувається анонімно (оскільки IP-адреси недоступні публічно), отже, користувачі можуть спілкуватися без особливих побоювань і державного втручання [4]. Саме тому даркнет часто сприймають як інструмент для здійснення комунікації в різних підпіллях і незаконній діяльності [5]. У більш загальному сенсі термін «даркнет» можна використати для опису некомерційних «вузлів» Інтернету [6] або віднести до всіх «підпільних» інтернет-комунікацій і технологій, які переважно пов'язані з незаконною діяльністю або інакомисленням.

Чорні ринки даркнету продають свої товари і послуги анонімним клієнтам, які часто розплачуються біткоїнами. Один з найбільших маркетів даркнету – Alphabay Market. У даркнеті доступні різні види наркотичних препаратів – близько 70 %. Також можна купити акаунти в соцмережах, персональну інформацію і сканування паспортів, різні документи – від номерів паспорту до водійських прав. Розповсюдженим товаром у даркнеті є скановані копії кредитних карт, які використовуються для картингу – викрадення коштів з цих карт [7]. Популяризація і відносна відкритість сервісу даркнету надає поштовх для ще більшого використання криптовалют, які дають можливість легко легалізувати кошти, отримані від зайняття злочинною діяльністю. Для прикладу розглянемо той факт, що будь-який користувач мережі біткоїн може створити будь-яку кількість адрес без ідентифікації. Транзакції між двома адресами, обидва з яких контролюються однією і тією самою людиною, не відрізняються від операцій, в яких різні люди контролюють ці адреси. Отже, теоретично зловмисники можуть провести, наприклад, 100 000 Bitcoin-транзакцій між адресами, які ними ж і контролюються, перед тим, як перетворити біткоїн в іншу форму. Відновлення такого ланцюга операцій, особливо якщо це робиться вручну, зайняло б надто багато часу, якби взагалі виявилося можливим. Такий прийом може бути частиною складної схеми з відмивання грошей з використанням декількох осіб, віртуальних валют. Так само, як і первинна торгівля віртуальними валютами, яка відбувається з адміністраторами або біржами віртуальних валют, вторинна торгівля віртуальними валютами, як, наприклад, під час використання інтернет-аукціонів або інших торгових майданчиків, також створює сприятливі можливості для збільшення складності проведення розслідування транзакцій [8]. Відповідно до результатів дослідження, проведеного ООН упродовж одного року, в світі відмивається в результаті здійснення різних кримінальних правопорушень грошових коштів у розмірі 2–5 % світового ВВП, що становить від 800 млрд до 2 трлн дол. США [9].

Якщо описувати криптовалюти з кримінологічної точки зору як засіб вчинення кримінального правопорушення, то варто зазначити такі особливості:

– швидкість обробки операції;

– анонімність власника або особи, яка оперує даними;

– значна кількість ланцюгів заплутаних транзакцій;

– доступ до активів з будь-якої точки земної кулі за допомогою Інтернету;

– зручність у перевезенні;

– відсутність повноцінного контролю та регулювання з боку органів влади багатьох країн.

Узагальнюючи кримінологічні особливості, можливо зробити невеликий висновок: використання криптовалюти – майже ідеальний засіб для вчинення або фінансування кримінально-протиправних діянь.

Також останнім часом спостерігається тенденції щодо популяризації використання віртуальних валют у протиправних фінансових схемах, спрямованих на легалізацію доходів, одержаних злочинним шляхом, у переважній більшості отриманих у готівковій формі. Так, особливо поширеним є факт використання криптовалют організованими злочинними угрупованнями як інструменту протиправної діяльності, пов'язаної із шахрайськими діями у сфері ІТ-технологій так званих «фінансових пірамід» [10].

Варто зазначити, що наразі в Україні діє воєнний стан, який був введений Указом Президента України від 24.02.2022 № 64/2022 [11] та затверджений Законом України «Про затвердження Указу Президента України «Про введення воєнного стану в Україні» 24.02.2022 № 2102-IX [12].

З метою запобігання витоку капіталу, було прийнято рішення щодо обмеження, а в деяких випадках і заборони транскордонних валютних операцій з українських банків на рахунки іноземних фінансових установ, а також операцій, пов'язаних купівлею, обміном електронних валют, поповненням електронних гаманців, тобто всі операцій, які передбачають роботу з іноземною валютою в режимі своп, P2P-перекази та операції quasi cash. Ці обмеження стосуються не тільки для утримання фінансової стабільності та захищеності України, а й попереджують фінансування ворожих диверсійних груп та терористичних псевдоутворень [13]. Рішення Правління НБУ від 4 березня 2022 року № 36, у редакції постанова Правління Національного банку України від 21 березня 2022 року № 58, від 4 квітня 2022 року № 68, від 20 квітня 2022 року (Київ № 78), змогли значно призупинити виток капіталу з України. Оскільки з початку повномасштабного вторгнення росії в Україну і до 20 квітня 2022 року за підрахунками НБУ з України було виведено близько 3 млрд доларів США.

Висновки. Чинні обмеження з боку держави доволі сильно вплинули на злочинний світ, а особливо наркотичний бізнес, тому що більшість операцій з купівлі та продажу наркотичних засобів і їх прекурсорів відбувається в електронній валюті. Звісно, система обмежень НБУ не є ідеальною, оскільки вона не регулює безпосереднє створення криптовалюти та її переміщення на персональні криптогаманці. Однак заборона купівлі та конвертації значно ускладнює злочинні процеси і на деякий час майже повністю зриває налагоджений злочинний конвеєр. На жаль, одними методами обмеження злочинність побороти не вдасться, оскільки досі залишається відкритим питання способу отримання електронної валюти, тому що нині одним з найпопулярніших методів її отримання є самовільне та незаконне під'єднання до електронних мереж як місцевого значення, так і стратегічної. А щодо обігу криптовалюти в осіб, які не є представниками злочинного світу, зазначимо, що

обмеження породжують бажання їх обходити будь-яким способом. Якщо влада країни зі стратегічною ціллю бажає уникнути масового витоку іноземної валюти, треба запроваджувати рішення, які не будуть спонукати людей шукати методи обходу обмежень та бажання вивести кошти, обіг як іноземної, так і електронної валюти, їх конвертування може давати можливість країні отримувати комісію за здійснення таких видів транзакцій. Заборона обороту валют не дає фінансову користь, на відміну від контрольованого обігу. У такий важкий час Україна потребує додаткових пасивних надходжень для того, щоб компенсувати заморожені надходження з тимчасово окупованих регіонів та якнайшвидше перемогти агресора.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Криптовалюта (від англ. Cryptocurrency). URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%D0%BB%D1%8E%D1%82%D0%B0 (дата звернення: 20.02.2022).

2. Гребенюк М. В., Лук'янчук Р. В. Правовий режим криптовалют: досвід ЄС. *Науковий вісник Національної академії внутрішніх справ*. 2017. С. 311.

3. Скришевич О. Криптовалюта як складова корупційних кримінальних правопорушень: новели законодавства. *Реалізація державної антикорупційної політики в міжнародному вимірі:* матеріали VI Міжнар. наук.-практ. конф., Київ, 9–10 груд. 2021 р. / редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ: НАВС, 2021. 484 с.

4. Wood, Jessica (2010). The Darknet: A Digital Copyright Revolution. Richmond Journal of Law and Technology[en] 16 (4): 15–17.

5. На темной стороне интернета: Что такое Dark Web и Deep Web? URL: https://www.dgl.ru/technology/internet/na-temnoy-storone-interneta-chto-takoe-dark-web-i-deep-web_11677.html (дата звернення: 21.02.2022).

6. Lasica J. D. Darknet: Hollywood's War Against the Digital Generation. Університет Каліфорнії: Hoboken, N.J.: Wiley, 2005. 320 с. ISBN 978-0471683346.

7. Карапетян О., Білинський В. Злочинні технології збагачення з використанням криптовалют та особливості їх розслідування. *Актуальні проблеми правознавства.* 2018. Випуск 2 (14).

8. Bal A. How to Tax Bitcoin? // Handbook of Digital Currency. Singapore, 2015. Pp. 267–282.

9. Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets // FATF, Paris, France: сайт. 2020. URL: www.fatf-gafi.org/publications/fatfrecommendations/documents/VirtualAssets-Red-Flag-Indicators.html (дата звернення: 29.08.2021).

10. Казначеєва Д. В., Дорош А. О. Кримінальні правопорушення у сфері обігу криптовалюти. *Вісник Кримінологічної асоціації України*. 2021. № 2 (25). С. 149–157.

11. Указ Президента України від 24.02.2022 № 64/2022 URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text (дата звернення: 01.05.2022).

12. Про затвердження Указу Президента України «Про введення воєнного стану в Україні»: Закон України від 24.02.2022 № 2102-IX. URL: https://zakon.rada.gov.ua/laws/show/2102-20#Text (дата звернення: 01.05.2022).

13. Про роботу банківської системи в період запровадження воєнного стану: Постанова Правління Національного банку України 24 лютого 2022 року № 18 (зі змінами, унесеними постановами Правління Національного банку України). Київ. URL: https://bank.gov.ua/admin_uploads/law/Resolution_24022022_18_kp.pdf (дата звернення: 01.05.2022).

REFERENCES

1. Cryptocurrency (from the English. Cryptocurrency). URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0 % B2% D0% B0% D0% BB% D1% 8E% D1% 82% D0% B0 (application date: 20.02.2022).

2. *Scientific Bulletin of the National Academy of Internal Affairs* © Grebenyuk MV, Lukyanchuk RV, 2017 310 INTERNATIONAL EXPERIENCE UDC 354.21: 336.457 Grebenyuk MV - LEGAL REGIME OF CRYPTOVALUT: EXPERIENCE11 EU / c. 3 EU.

3. *Implementation of state anti-corruption policy in the international dimension*: materials of the VI International. Nauk.-prakt. Conf. (Kyiv, December 9–10, 2021) / [editor: c. V. Cherney, village D. Gusarev, village S. Chernyavsky and others]. Kyiv: Nat. Acad. Inside. Sprav, 2021. 484 O. Skryshevych, Professor of the Department of Criminal Law of the National Academy of Internal Affairs, Candidate of Law, Professor of Cryptocurrency as a Component of Corruption Criminal Offenses: Novelties of Legislation.

4. Wood, Jessica (2010). The Darknet: A Digital Copyright Revolution. Richmond Journal of Law and Technology [en] 16 (4): 15–17.

5. On the dark side of the Internet: What is the Dark Web and the Deep Web? URL: https://www.dgl.ru/technology/internet/na-temnoy-storone-interneta-chto-takoe-dark-web-i-deep-web_11677.html (accessed: 21.02.2022).

6. J. D. Weasel. "Darknet: Hollywood's War Against the Digital Generation". University of California: Hoboken, N.J.: Wiley, 2005. 320 p. ISBN 978-0471683346.

7. Criminal Enrichment Technologies Using Cryptovalutes and Features of Their Investigation. Karapetyan O., Bilinsky V., ISSN 2524-0129. *Current issues of jurisprudence*. Issue 2 (14). 2018.

8. Bal A. How to Tax Bitcoin? // Handbook of Digital Currency.Singapore, 2015. Pp. 267–282.

9. Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets // FATF, Paris, France: сайт. 2020. URL: www.fatf-gafi.org/publications/fatfrecommendations/documents/VirtualAssets-Red-Flag-Indicators.html (accessed: 29.08.2021).

10. Kaznacheeva, D. V., Dorosh A. O. Criminal offenses in the field of cryptocurrency circulation. *Bulletin of the Criminological Association of Ukraine*. 2021. № 2 (25). P. 149–157.

11. Decree of the President of Ukraine of 24.02.2022 № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text (date of application: 01.05.2022).

12. Law of Ukraine On Approval of the Decree of the President of Ukraine "On the Imposition of Martial Law in Ukraine" 24.02.2022 № 2102-IX. URL: https://zakon.rada.gov.ua/laws/show/2102-20#Text (date of application: 01.05.2022).

13. RESOLUTION of the Board of the National Bank of Ukraine February 24, 2022 Kyiv № 18. On the operation of the banking system during martial law (as amended by the Board of the National Bank of Ukraine). URL: https://bank.gov.ua/admin_uploads/law/ Resolution_24022022_18_kp.pdf (application date: 01.05.2022).

D. Chaikovskyi. Criminological aspects of crime prevention related to the USE of non-cash assets (cryptocurrencies)

The XXI century is characterized by the rapid development of modern information technologies, which are becoming more perfect every day and the volume of data processing is growing. Information resources currently consist not only of data but also of funds, namely electronic currencies and non-cash resources that travel from one e-wallet to another.

The purpose of article is identify and investigate criminological aspects of crime prevention related to the use of non-cash assets (cryptocurrency). Highlight your own theoretical vision of the approach to crime prevention using electronic currency.

The use of electronic currencies in the criminal sphere is quite relevant and widespread, as it allows anonymous financing and income from criminal activities, as cryptocurrency is by nature endowed with a certain confidentiality and carries almost no information about its owner. The XXI century is characterized by the rapid development of modern information technologies, which are becoming more perfect every day and the volume of data processing is growing. Information resources currently consist not only of data but also of funds, namely electronic currencies and non-cash resources that travel from one e-wallet to another.

Methods. Information-analytical, formal-legal, comparative and inductive methods were used in writing the research.

Highlight your own theoretical approach to preventing crime related to the use of non-cash assets (cryptocurrency), improve existing methods of preventing this type of crime.

The current restrictions on the part of the state have had a significant impact on the criminal world, especially the drug business, because most transactions in the purchase and sale of drugs and their precursors take place in electronic currency. Of course, the NBU's system of restrictions is not ideal, as it does not regulate the direct creation of cryptocurrency and its transfer to personal crypto-wallets. However, the ban on buying and converting significantly complicates criminal proceedings and for some time almost.

Keywords: *non-cash assets, blockchain, electronic currency, crime prevention, counteraction, cryptocurrency, cross-border currency transactions.*

Стаття надійшла до редколегії 12 травня 2022 року