1929)". In P. Berger, G. Bischof, & F. Plasser (Eds.), From Empire to Republic: Post-World War I Austria. Vol. 19, pp. 370-398, University of New Orleans Press. [Online], available at: https://doi.org/10.2307/j.ctt1n2txcs.20 (Accessed 23 April 2024).

9. Tomka, B. and Szikra, D. (2009). Social Policy in East Central Europe: Major Trends in the 20th Century. [Online], pp. 17-34, available at: https://www.researchgate.net/publication/259165355_Social_Policy_in_East_Central_Europe_Major_Trends_in_the_20th_Century (Accessed 23 April 2024).

10. Brenk, M., Chaczko, K. and Pląsek, R. (2018). "100 years of the social assistance system in Poland", Biuletyn Historii Wychowania, [Online], available at: https://doi.org/10.14746/bhw.2018.39.10 (Accessed 23 April 2024).

11. Rimlinger, Gaston V. (1971). Welfare Policy and Industrialization in Europe, America, and Russia. Wiley, New York, USA.

12. Part XIII of the Treaty of Peace of Versailles // International Labour Office. Official Bulletin. Volume I. April 1919-August 1920. [Online], available at: https://www.ilo.org/wcmsp5/groups/public/---dgreports/---jur/documents/genericdocument/wcms_441862.pdf (Accessed 23 April 2024).

13. Pensijne zabezpechennia v Ukraini ta Bilorusi: istoriia stanovlennia i perspektyvy rozvytku [Pension provision in Ukraine and Belarus: the history of formation and the prospects of development] (2018), edited by: Shumylo, M.M. and Komotskaya I.O., Nika-Center, Kyiv, Ukraine.

14. The new constitutions of Europe / Howard Lee Mc Bain and Lindsay Rogers. - Garden City, 1922. – 640 p. [Online], available at: https://books.google.com.ua/books?id=zEwpAAAAYAAJ&pg=PA401&source=gbs_toc_r&cad=3#v=onepage&q&f=false (Accessed 23 April 2024).

15. Frantsuz A.J. (2015) "The Strengthening and Ensuring of Human rights as Defining Determinant of Ukraine's Political System", Scientific Journal of Lviv State University of Internal Affairs. Law. Vol. 2, pp. 66-77.

16. The official site of Social Insurance Institution (2023), "Social security in Poland" available at: https://www.zus.pl/documents/10182/167615/Social+Security+in+Poland/71ffe1b1-c142-48fa-a67b-0c7e1cec6eb6 (Accessed 23 April 2024).

Стаття надійшла до друку 25 квітня 2024 року

УДК 343.9
DOI - 10.31732/2708-339X-2024-12-A12

СВІТОВИЙ ДОСВІД ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ, ПОВ'ЯЗАНИМ З ОБІГОМ ВІРТУАЛЬНИХ АКТИВІВ

Доляновська І.М.,
кандидат юридичних наук, доцент
Університет «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: DolianovskaIM@krok.edu.ua
ORCID: https://orcid.org/0000-0002-1606-7096

Кривенко К.О.,
аспірант Університету «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: KryvenkoKO@krok.edu.ua
ORCID: https://orcid.org/0009-0006-1327-757X

GLOBAL EXPERIENCE IN COMBATING CRIMINAL OFFENCES RELATED TO THE CIRCULATION OF VIRTUAL ASSETS

Dolianovska I.M.,
Ph.D. in Law, Associate Professor «KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: DolianovskaIM@krok.edu.ua
ORCID: https://orcid.org/0000-0002-1606-7096

ISSN (Print) 2708-339X ISSN (Online) 2786-7498
Legal Bulletin № 2 (12), 2024
Kryvenko K.O.,
PhD student «KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: KryvenkoKO@krok.edu.ua
ORCID: https://orcid.org/0009-0006-1327-757X

Анотація*. Стаття здебільшого присвячена ґрунтовному аналізу та кримінологічній характеристиці кримінальних правопорушень у сфері обігу віртуальних активів, а також безпосередньо протидії таким кримінальним правопорушенням. Аналіз кримінальних правопорушень базується виключно на світовому досвіді виявлення та розслідування даної категорії протиправних дій. У процесі дослідження надано характеристику категорії кримінальних правопорушень у сфері обігу віртуальних активів. Так, кримінальні правопорушення у сфері обігу віртуальних активів включають різноманітні склади злочинів, безпосереднім предметом або засобом вчинення яких виступають віртуальні активи.*

Виділено умовну класифікацію кримінальних правопорушень, пов'язаних з обігом віртуальних активів через призму їх ролі у вчиненні кримінальних правопорушень, а саме: безпосереднє заволодіння віртуальними активами; легалізація доходів, отриманих злочинним шляхом за допомогою використання віртуальних активів; торгівля забороненими товарами та послугами, де засобом платежу виступають віртуальні активи.

Досліджено відомості про реальні факти вчинення кримінальних правопорушень, у тому числі витримки з вироків іноземних судів, в яких здійснено опис встановлених фактичних обставин справи. У процесі дослідження встановлено основні чинники запобігання та протидії вказаній категорії кримінальних правопорушень, серед яких: розробка та втілення правового регулювання обігу віртуальних активів; співпраця між правоохоронними органами та учасниками ринку (криптобіржами, аналітичними центрами та іншими сервісами); впровадження та використання правоохоронними органами спеціальних інструментів відстеження транзакцій; міжнародна співпраця між правоохоронними органами та інше.

На прикладі практичних кейсів прослідковано розвиток засобів та методів правоохоронних органів щодо боротьби зі злочинністю, яка використовує віртуальні активи в якості засобу платежу за нелегальні товари та послуги. Визначено основні напрями для розвитку українських правоохоронних органів шляхом перейняття успішного досвіду іноземних колег щодо виявлення та припинення кримінальних правопорушень, пов'язаних з обігом віртуальних активів.

Ключові слова: *«віртуальні активи», «криптоактиви», «криптовалюта», «цифрові активи», «правове регулювання обігу вірутальних активів».*

Формул*: 0, рис.: 0, табл.: 0, бібл.:8.*

Abstract*. This article primarily focuses on a thorough analysis and criminological characterization of criminal offenses related to virtual assets trafficking, as well as the direct counteraction to such offenses. The analysis is based exclusively on global experiences in detecting and investigating this category of unlawful acts. The author describes the category of criminal offenses in the field of virtual assets trafficking, which includes various corpus delicti where the direct object or means of commission involves virtual assets.*

A conditional classification of these offenses is proposed, viewed through the lens of their role in criminal activities, namely: direct seizure of virtual assets; legalization of proceeds of crime using virtual assets; and trading in prohibited goods and services with virtual assets as a means of payment. The author examines information on criminal offenses, including excerpts from foreign court judgments that detail the established factual circumstances of the cases.

The study identifies key factors for the prevention and counteraction of this category of criminal offenses, including the development and implementation of legal regulations governing virtual asset circulation; cooperation between law enforcement agencies and market participants (such as crypto exchanges and analytical centers); the introduction and utilization of special transaction tracking tools by law enforcement; and international cooperation among law enforcement agencies.

Additionally, the author traces the evolution of methods used by law enforcement to combat crimes involving virtual assets as a means of payment for illegal goods and services, illustrated through practical case examples. The main directions for the development of Ukrainian law enforcement agencies are identified, emphasizing the adoption of successful practices from foreign counterparts in detecting and suppressing offenses related to virtual asset circulation.

Keywords*: virtual assets, cryptoassets, cryptocurrency, digital assets, legal regulation of virtual asset circulation.*

Formulas*: 0, fig.: 0, tabl.: 0, bibl.: 8.*

Постановка проблеми. Віртуальні активи з кожним днем стають частиною повсякденного життя все більшої кількості пересічних громадян. Наша держава не лише не є виключенням у цьому процесі, а й займає одне з лідерських місць у світі з використання криптоактивів серед населення. Попри це, українське законодавство досі не має належного правового регулювання обігу віртуальних активів, на відміну від Європейського союзу та США, які не лише врегулювали «правила гри» на ринку вірту-

альних активів, а й почали активну боротьбу з їх незаконним обігом та використанням у злочинних цілях. Використовуючи криптовалюти, можна придбати широкий спектр нелегальних товарів і послуг. Віртуальні гроші використовуються в порноіндустрії, у сфері незаконного обігу персональних даних, у торгівлі підробленими документами, нелегальними ліками, і навіть криптовалютою оплачують замовні вбивства» [1].

Аналіз останніх досліджень. Загальні питання правового регулювання віртуальних активів в Україні та світі ставали предметом дослідження у працях Р. Майданика [2], Л. Тимченко [3], Т. Гудіми [3] та інших. Окремі питання використання віртуальних активів у протиправній діяльності розглядались у наукових працях В. Бохенка [5], Д. Казначеєвої [1] та інших.

Не вирішені раніше частини загальної проблеми. Аналізуючи праці вищезазначених вчених, а також наявну нормативну базу, вимушені констатувати, що незважаючи на намагання законодавця врегулювати обіг віртуальних активів в Україні, остаточного вирішення щодо цього питання наразі так і не прийнято. Що стосується саме виявлення та протидії кримінальних правопорушень у цій сфері, то цьому питанню ані на нормативному, ані на теоретичному рівнях не приділяється належної уваги, що сприяє розвитку нелегального обігу віртуальних активів в нашій державі.

Формулюванні цілей статті. Задля того, щоб наздогнати розвинуті країни та перейняти досвід виявлення та розкриття кримінальних правопорушень у сфері обігу віртуальних активів у практику діяльності українських правоохоронних органів, виникає об'єктивна необхідність у дослідженні передового досвіду правоохоронних органів США, країн Європейського союзу, а також міжурядових організацій з цього питання. Основною метою дослідження у цій статті є правовий аналіз виявлених кримінальних правопорушень у сфері обігу віртуальних активів, визначення ознак цієї категорії кримінальних правопорушень, аналіз виявлення та протидії, а також розробка рекомендацій щодо впровадження в Україні досвіду іноземних правоохоронних органів по виявленню та розкриттю кримінальних правопорушень у сфері обігу віртуальних активів.

Виклад основного матеріалу. Масове прийняття використання віртуальних активів в Україні та світі збільшується з кожним роком. За результатами дослідження відомої аналітичної компанії «Chainalysis», Україна у 2023 році зайняла п'яте місце у глобальному рейтингу сприйняття криптовалют [7]. Це свідчить про те, що українці дедалі частіше використовують віртуальні активи у повсякденному житті, зокрема як спосіб інвестування, зберігання коштів, переказу коштів, торгівлі на криптобіржах, а також розрахунку за товари та послуги.

Глобальне користування криптоактивами обумовлене їх властивостями, такими як швидкість транзакцій, незначна комісія, легкість у використанні та інші. Однак, поряд з корисними властивостями криптовалют, існують також й ті, що можуть бути використані у вчиненні неправомірних дій. Йдеться у першу чергу про відносну анонімність учасників транзакцій, децентралізацію та технологічні властивості щодо заплутування відстеження переказів.

Криптовалюта є конвертованою, децентралізованою, віртуальною, конфіденційною, цифровою та нефіатною, відповідно вона не є електронними грошима, які випускаються офіційним державним емітентом [3]. Такі особливості новітніх технологій не залишились поза увагою кримінального світу, представники якого завжди відзначались слідуванням у ногу з часом та запозиченням технологій у протиправну діяльність. Розповсюдженими прикладами використання криптовалюти у протиправній діяльності є використання її в якості засобу платежу при незаконному обігу наркотичних та психотропних речовин, торгівлі зброєю, персональними даними, фінансуванні тероризму, а також торгівлі людьми та органами. Разом з цим, віртуальні активи можуть бути й предметом кримінальних правопорушень, зокрема: відмивання коштів, корупційних кримінальних правопорушень, шахрайства, крадіжки, заволодіння, вимагання, а також злочинів, пов'язаних з несанкціонованим втручанням в роботу комп'ютерів та мереж. Таким чином, можемо виділити нову категорію кримінальних правопорушень, пов'я-

заних з обігом віртуальних активів, до якої увійдуть усі вищезгадані склади кримінальних правопорушень, у випадку вчинення їх з використанням або щодо віртуальних активів.

Разом з цим, доцільним буде класифікувати кримінальні правопорушення, пов'язані з обігом віртуальних активів на наступні категорії: кримінальні правопорушення, пов'язані з безпосереднім заволодінням криптоактивами; кримінальні правопорушення, де криптоактиви використовуються для легалізації коштів та інших активів, отриманих злочинним шляхом; кримінальні правопорушення, в яких криптоактиви використовуються в якості засобу платежу за нелегальні товари та послуги.

Варто відзначити, що ще з 2018 року Група з розробки фінансових заходів боротьби з відмиванням грошей (FATF) підіймає гостро проблему використання віртуальних активів у протиправній діяльності. Так, країнам та фінансовим установам надано рекомендації щодо виявлення та оцінювання ризиків відмивання коштів або фінансування тероризму, які можуть виникати у зв'язку з (а) розробкою нових продуктів та нових напрямків діяльності, включаючи нові механізми постачання, та (б) використанням нових технологій або тих, що розвиваються як для нових, так і для вже існуючих продуктів. Для управління та зменшення ризиків, пов'язаних з віртуальними активами, країнам було рекомендовано забезпечити, щоб постачальники послуг з віртуальних активів для цілей регулювання сфери ПВК/ФТ, ліцензували чи реєстрували діяльність і підпорядковувались ефективним системам моніторингу та забезпечували відповідність заходам, які передбачені Рекомендаціями FATF [8].

На жаль, до сьогодні Україна так і не спромоглась побудувати та втілити належний правовий механізм регулювання обігу віртуальних активів на своїй території, а відтак маємо констатувати, що в Україні одні з найсприятливіших умов для використання віртуальних активів у нелегальної діяльності. Адже дозволено все те, що не заборонено законом. Тому, як справедливо зазначає В. Бохенко: «Правова неврегульованість і невизначеність статусу криптовалют у більшості країн світу значно ускладнює не тільки нагальну оцінку її використання під час кваліфікації таких дій, але й також гальмує розкриття та розслідування злочинів, під час скоєння яких використовується криптовалюта або як предмет злочину, або як засіб скоєння кримінального правопорушення. Таким чином, з метою ефективної протидії злочинності у сфері обігу криптовалют правоохоронцям необхідно більш детально і всебічно опанувати процеси та явища, які можуть мати опосередкований або виражений негативний вплив на обіг криптовалют» [5]. Подібної думки дотримується і Доляновська І.М., яка, досліджуючи попередження правопорушень у сфері дотримання прав людини, зазначає, що «…одним із шляхів боротьби із правопорушеннями є власне попередження вчинення правопорушень…» [6].

У відкритих джерелах міститься інформація про виявлення всього лише декількох незначних кримінальних правопорушень в Україні, де тим чи іншим чином фігурують віртуальні активи. Здебільшого ці кримінальні правопорушення пов'язані з шахрайством, вимаганням або торгівлею наркотичними та психотропними речовинами.

Поряд з цим, світовий досвід свідчить про виявлення більш значних кримінальних правопорушень у сфері обігу віртуальних активів, зокрема: заволодіння віртуальними активами на суму в декілька мільярдів доларів США, використання багаторівневих ланцюгів для відмивання коштів, отриманих злочинним шляхом за допомогою властивостей віртуальних активів та інше.

Задля встановлення випадків використання технологій та новацій, пов'язаних з віртуальними активами у злочинній діяльності, необхідно проаналізувати світову практику виявлення та розслідування кримінальних правопорушень, де фігурують віртуальні активи.

Так найбільш відомим зломом в історії криптовалют залишається отримання несанкціонованого доступу до однієї з перших криптобірж під назвою «Mt.Gox», тобто її злом. Як вбачається з відкритих джерел, на початку 2014 року на платформу приходилось близько 70% від загального об'єму тор-

гівлі біткоїном. Протягом 2011-2013 років зловмисникам вдалося непомітно вивести з біржі 650 000 BTC, що станом на теперішній час складає близько $45 млрд (на момент злому близько $440-480 млн).

Організаторів та виконавців злому біржі так й не було встановлено, а за результатами розслідування, злом «Mt.Gox» відбувся через низький рівень безпеки платформи та багаточисельні помилки менеджменту біржі [9].

Окружний суд Токіо визнав винним колишнього головного виконавчого директора (CEO) біржі «Mt.Gox» в підробці документів і засудив його до двох років і шести місяців позбавлення волі з умовним терміном на 4 роки. Цікавим є той факт, що сторона обвинувачення кваліфікувала дії CEO біржі як розкрадання та порушення корпоративного права, у зв'язку з чим просила суд про покарання у вигляді 10 років позбавлення волі, проте за цими звинуваченнями його було визнано невинним [10].

Другим кричущим випадком злому криптобіржі є злом блокчейн-платформи «Poly Network», яка стала однією з найбільших крадіжок у сфері децентралізованих фінансів (DeFi) [11]. DeFi – це фінансова технологія, заснована на захищених розподілених реєстрах. Це середовище, яке дає змогу використовувати фінансові послуги без необхідності покладатися на централізовані організації. У системі DeFi фінансові послуги надаються через децентралізовані додатки (dApps), більшість з яких розгорнуто на платформі Ethereum [12].

За наявної інформації, 10 серпня 2022 року хакери здійснили несанкціоноване втручання в роботу «Poly Network» та вивели криптовалюти на суму понад $600 млн. Проте, незабаром після крадіжки хакери почали добровільно повертати викрадені активи. Аналітики припускають, що зловмисники не змогли відмити та легалізувати викрадені криптоактиви через прозорість блокчейну та використання аналітичних інструментів фінансовими установами, хоча сам хакер заявив, що зробив це заради розваги та гроші його не цікавлять [11].

Розглянуті практичні приклади умисних дій зловмисників, направлених на заволодіння криптоактивами свідчать про появу нових загроз у кібербезпеці, а відтак й нових викликів для правоохоронних органів. Внаслідок заволодіння криптоактивами окремо кваліфікуються дії викрадачів та адміністраторів інтернет-ресурсів, через дії або бездіяльність яких допущено несанкціоноване втручання до системи та викрадення активів.

Світовий досвід свідчить про наявність певного прогресу в виявленні та розслідуванні кримінальних правопорушень, пов'язаних зі світом віртуальних активів. Так, у випадку з криптобіржею «Mt.Gox» злочин, вчинений у 2012-2014 роках так й не був розкритий через певні властивості новітньої технології та необізнаності правоохоронних органів з методами та засобами протидії новій категорії кримінальних правопорушень. Тому прокуратура обмежилась висуненням обвинувачення службовій особі криптобіржі. У другому ж випадку, який стався у 2022 році, для уникнення викриття, зловмисники замаскували злом під перевірку кібербезпеки та погодились повернути викрадене [10, 11].

Незважаючи на кінцевий результат, обидва випадки свідчать про появу та розвиток нової категорії кримінальних правопорушень, пов'язаних з заволодінням віртуальними активами, а також про формування нового суб'єктного портрету злочинця, тобто особи, яка має спеціальні знання та навички у сфері написання комп'ютерного коду та використання програмного забезпечення, метою якого є викрадення віртуальних активів. Важливо також звернути увагу, що психологічний портрет особи, яка вчиняє такого роду кримінальне правопорушення, відрізняється психологічного портеру злочинця у класичному розумінні.

Ще одним випадком протиправного заволодіння криптоактивами та успішного виявлення і конфіскації цих активів правоохоронними органами стала справа криптобіржі «Bitfinex». Відповідно до відкритих джерел, злом кртиптобіржі стався у 2016 році, коли хакери здійснили несанкціонований доступ до біржі, запустили 2072 несанкціонованих транзакцій, внаслідок чого вивели з біржі в загальній кількості майже 120 тисяч BTC, що належали користувачам. Вказаний злом не лише спричинив майнову

шкоду власникам викрадених віртуальних активів, а й вплинув на зменшення ринкової вартості першої криптовалюти майже на 20%.

Як слідує з опублікованих документів, слідство тривалий час не мало змоги встановити зловмисників через те, що після виведення криптоативів з біржі на сторонній криптовалютний гаманець, останні майже не користувалися ними, адже розуміли, що прозорість технології блокчейн не дасть змоги просто вивести кошти та розпорядитися ними. Зловмисники, розуміючи всі ризики виявлення, діяли дуже обережно та добре планували свої дії. Частина викрадених криптоактивів згодом все ж таки була виведена у фіат, переважно за допомогою онлайн-маркетів для торгівлі нелегальними товарами «AlphaBay» та «Hydra», а також шляхом використання інших сервісів та бірж.

Більша частина справи залишається засекреченою, але з опублікованих документів та прес-релізів правоохоронних органів встановлено, що розслідування у справі щодо заволодіння віртуальними активами «Bitfinex» внаслідок несанкціонованого доступу, активізувалось після того, як Федеральне бюро розслідувань припинило діяльність нелегального сервісу «AlphaBay» та отримало доступ до акаунтів користувачів, в результаті чого й було виявлено можливих зловмисників. У подальшому, на підставі ордеру суду, детективами у ході обшуку було отримано доступ до хмарного сховища одного з підозрюваних, де й було виявлено паролі від криптовалютних гаманців, на які було виведено криптоактиви з біржі «Bitfinex», де перебувало 94 643 BTC. За результатами розслідування, у 2022 році було арештовано двох осіб, яким висунули обвинувачення у злочинній змові з метою відмивання коштів, одержаних злочинним шляхом. На підставі угод про визнання винуватості, обвинуваченим було погоджено покарання у вигляді 20 та 10 років позбавлення волі. Цікаво, що сторона обвинувачення не знайшла доказів того, що саме ці особи причетні до зламу біржі, а тому обвинувачення за цим фактом висунуте не було. Разом з цим, відбулось безпрецедентне застосування конфіскації виявлених біткоїнів, загальна вартість яких наразі складає близько $6 млрд, частина з яких направлена на відшкодування шкоди користувачів біржі [13].

Розглянутий випадок дає можливість зробити висновок як щодо розвитку методів розслідування та прогресування іноземних правоохоронних органів у цьому напрямку, так й щодо виняткової складності розслідування новітньої категорії кримінальних правопорушень, що потребує опанування правоохоронним органам технологій та нових знань.

Для прикладу, в США вже створена та успішно діє Національна група з питань криптовалют (NCET) Секції комп'ютерних злочинів та інтелектуальної власності (CCIPS) Кримінального департаменту Мін'юсту США. Вона була створена для боротьби зі зростаючим незаконним використанням криптовалют та цифрових активів. За допомогою NCET проводяться розслідування щодо фізичних та юридичних осіб, які використовують цифрові активи для вчинення та сприяння вчиненню різноманітних злочинів, приділяючи особливу увагу біржам віртуальних валют, сервісам змішування та переведення грошей, а також провайдерам інфраструктури. NCET також встановлює стратегічні пріоритети щодо технологій цифрових активів, визначає сфери, які потребують підвищеної уваги з боку слідства та прокуратури, і очолює зусилля Кримінального департаменту Мін'юсту щодо співпраці з вітчизняними та іноземними державними установами, а також приватним сектором з метою активного розслідування та судового переслідування злочинів, пов'язаних з криптовалютами та цифровими активами [14].

Вищезазначене може свідчити про те, що обсяг та значимість кримінальних правопорушень у сфері обігу віртуальних активів в США дійшли такого рівня, що задля координації загальних зусиль у боротьбі з цим явищем було створено окрему інституцію.

У розглянутих вище випадках вчинення кримінальних правопорушень криптоактиви виступали переважно в якості предмету злочину, тобто ціллю зловмисників. Однак найбільш розповсюдженим у світі та в Україні, зокрема, залишається використан-

ня криптоактивів в якості засобу платежу за нелегальні товари та послуги.

У 2017 році Європол відрапортував про закриття двох найбільших кримінальних онлайн маркетів «AlphaBay» та «Hansa». «Дві великі правоохоронні операції під керівництвом Федерального бюро розслідувань (ФБР), Агентства США з боротьби з наркотиками (DEA) та Національної поліції Нідерландів за підтримки Європолу ліквідували інфраструктуру підпільної злочинної економіки, відповідальної за торгівлю понад 350 000 нелегальних товарів, включаючи наркотики, підроблені ідентифікаційні документи і пристрої доступу, контрафактні товари, шкідливе програмне забезпечення та інші інструменти для злому комп'ютерів, вогнепальну зброю і шахрайські послуги. За консервативними оцінками, з моменту створення ринку в 2014 році на ньому було здійснено транзакцій на суму в 1 мільярд доларів США. Транзакції оплачувалися в біткоїнах та інших криптовалютах. «Hansa» був третім за величиною кримінальним ринком у Darknet, на якому торгували такими ж великими обсягами заборонених наркотиків та інших товарів, – йдеться у офіційному прес-релізі Європолу [15].

Висновки. Проаналізовані випадки фігурування криптоактивів у злочинній діяльності, а також світова практика виявлення та боротьби з цим явищем свідчить про активне використання новітніх технологій у протиправній діяльності. Поряд з використанням віртуальних активів для вчинення вже звичних кримінальних правопорушень, як вимагання, шахрайство та торгівля наркотиками, виникають також нові склади кримінальних правопорушень, такі як: заволодіння віртуальними активами, відмивання криптоактивів, отриманих злочинним шляхом, викрадення криптоактивів внаслідок несанкціонованого доступу до них та інші. З огляду на це, нашій державі також необхідно зосередити свою увагу на виявленні та протидії вказаній категорії кримінальних правопорушень. Окрім втілення відповідного регулюючого законодавства у сфері обігу криптоактивів, вкрай необхідним є також налагодження співпраці з правоохоронними органами США та Європи, перейняття їх успішного досвіду та впровадження освітніх програм, направлених на створення професійних кадрів у сфері боротьби з кримінальними правопорушеннями, пов'язаними з обігом віртуальних активів. Не зайвим буде створення з часом спеціального органу або установи, яка координуватиме зусилля інших контролюючих та правоохоронних органів у напрямку виявлення та протидії кримінальним правопорушенням у сфері обігу віртуальних активів.

Література:

1. Казначеєва Д.В. Основні види злочинів, що вчиняються із застосуванням криптовалюти. Протидія кіберзагрозам та торгівлі людьми: зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 26 листоп. 2019 р.). Харків: ХНУВС, 2019. С. 166-168

2. Майданик Р.А. Криптовалюта: проблеми правового регулювання. Актуальні проблеми приватного права: матеріали наук.-практ. конф., присвяч. 96-й річниці з дня народж. В. П. Маслова (м. Харків, 14 лют. 2018 р.). Харків: Право, 2018. С.11-15.

3. Тимченко Л.М., Хмеленко К.М. Загальна характеристика криптовалюти. URL: https://doi.org/10.32782/2524-0374/2022-12/80 (дата звернення: 20.04.2024).

4. Гудіма Т.С., Устименко В.А., Джабраілов Р.А., Черних О.С. Особливості правового регулювання обігу віртуальних активів в Україні: Де-факто vs Де-юре. Financial and credit activity problems of theory and practice. 5, 46 (Жов 2022), 137-148. URL: https://doi.org/10.55643/fcaptp.5.46.2022.3844.

5. Бохенко В.М. «Кримінологічні ризики обігу криптовалют». URL: https://doi.org/10.32782/2524-0374/2021-12/82 (дата звернення: 20.04.2024).

6. Доляновська І.М. «Співробітництво Організації Об'єднаних Націй та уряду України у сфері захисту прав дітей як напрям загальносоціального попередження злочинності: сучасні аспекти». URL: https://lbku.krok.edu.ua/index.php/legal-bulletin/article/view/356/297 (дата звернення: 20.04.2024).

7. The 2023 Global Crypto Adoption Index: Central & Southern Asia Are Leading the Way in Grassroots Crypto Adoption. URL: https://www.chainalysis.com/blog/2023-global-crypto-adoption-index/ (дата звернення: 20.04.2024).

8. Міжнародні стандарти щодо боротьби з відмиванням коштів, фінансуванням тероризму та розповсюдження зброї масового знищення. Рекомендації FATF. URL: https://fiu.gov.ua/assets/userfiles/books/5%20round%20FATF.pdf (дата звернення: 20.04.2024).

9. Breaking open the MtGox case, part 1. URL: https://blog.wizsec.jp/2017/07/breaking-open-mtgox-1.

html?m=1 (дата звернення: 20.04.2024).

10. Колишнього главу Mt.Gox визнано винним у підробці документів. URL: https://forklog.com/news/byvshij-glava-mt-gox-priznan-vinovnym-v-poddelke-dokumentov (дата звернення: 20.04.2024).

11. Хакер здійснив найбільший криптовалютний злом і повернув кошти. URL: https://finclub.net/ua/news/khaker-zdiisnyv-naibilshyi-kryptovaliutnyi-zlam-i-povernuv-koshty.html (дата звернення: 20.04.2024).

12. Що таке DeFi простими словами? URL: https://blog.whitebit.com/uk/what-is-defi-and-how-does-it-work/#heading-0 (дата звернення: 20.04.2024).

13. Bitfinex Hacker and Wife Plead Guilty to Money Laundering Conspiracy Involving Billions in Cryptocurrency. URL: https://www.justice.gov/opa/pr/bitfinex-hacker-and-wife-plead-guilty-money-laundering-conspiracy-involving-billions (дата звернення: 20.04.2024).

14. Two Foreign Nationals Arrested for Laundering at Least $73M Through Shell Companies Tied to Cryptocurrency Investment Scams. URL: https://www.secretservice.gov/newsroom/releases/2024/05/two-foreign-nationals-arrested-laundering-least-73m-through-shell (дата звернення: 20.04.2024).

15. Massive blow to criminal Dark Web activities after globally coordinated operation. URL: https://www.europol.europa.eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation (дата звернення: 20.04.2024).

References:

1. Kaznacheieva D.V. (2019) “The main types of crimes committed with the use of cryptocurrency. Counteracting Cyber Threats and Human Trafficking” Protydiia kiberzahrozam ta torhivli liud’my: zb. materialiv Mizhnar. nauk.-prakt. konf. pp. 166-168.

2. Majdanyk R.A. (2018) “Cryptocurrency: problems of legal regulation.” Aktual’ni problemy pryvatnoho prava: materialy nauk.-prakt. konf., prysviach. 96-j richnytsi z dnia narodzh. V. P. Maslova pp. 11-15.

3. Tymchenko L.M., Khmelenko K.M. (2022) “General characteristics of cryptocurrencies.” Yurydychnyj naukovyj elektronnyj zhurnal, [Online], vol. 12, available at: https://doi.org/10.32782/2524-0374/2022-12/80 (Accessed 20 April 2024).

4. Hudima T.S., Ustymenko V.A., Dzhabrailov R.A., Chernykh O.S. (2022) “Peculiarities of legal regulation of the circulation of virtual assets in Ukraine: De Facto vs De Jure.” Financial and credit activity problems of theory and practice. [Online], vol. 5 (46), available at: https://doi.org/10.55643/fcaptp.5.46.2022.3844 (Accessed 20 April 2024).

5. Bokhenko V.M. (2021) “Criminological risks of cryptocurrency circulation” Yurydychnyj naukovyj elektronnyj zhurnal, [Online], vol. 12, available at: https://doi.org/10.32782/2524-0374/2021-12/82 (Accessed 20 April 2024).

6. Dolianovska I.M. (2022) «Cooperation of the United Nations and the government of Ukraine in the field of protection of children’s rights as a direction of social crime prevention: modern aspects». URL: https://lbku.krok.edu.ua/index.php/legal-bulletin/article/view/356/297 (Accessed 20 April 2024).

7. “The 2023 Global Crypto Adoption Index: Central & Southern Asia Are Leading the Way in Grassroots Crypto Adoption” [Online], available at: https://www.chainalysis.com/blog/2023-global-crypto-adoption-index/ (Accessed 20 April 2024).

8. State Financial Monitoring Service of Ukraine (2018) “International standards for combating money laundering, terrorist financing and proliferation of weapons of mass destruction. FATF recommendations” [Online], available at: https://fiu.gov.ua/assets/userfiles/books/5%20round%20FATF.pdf (Accessed 20 April 2024).

9. “Breaking open the MtGox case, part 1” [Online], available at: https://blog.wizsec.jp/2017/07/breaking-open-mtgox-1.html?m=1 (Accessed 20 April 2024).

10. “Former head of Mt. Gox found guilty of forgery” [Online], available at: https://forklog.com/news/byvshij-glava-mt-gox-priznan-vinovnym-v-poddelke-dokumentov (Accessed 20 April 2024).

11. “Hacker makes the largest cryptocurrency hack and returns funds” [Online], available at: https://finclub.net/ua/news/khaker-zdiisnyv-naibilshyi-kryptovaliutnyi-zlam-i-povernuv-koshty.html (Accessed 20 April 2024).

12. “What is DeFi in simple terms?” [Online], available at: https://blog.whitebit.com/uk/what-is-defi-and-how-does-it-work/#heading-0 (Accessed 20 April 2024).

13. “Bitfinex Hacker and Wife Plead Guilty to Money Laundering Conspiracy Involving Billions in Cryptocurrency” [Online], available at: https://www.justice.gov/opa/pr/bitfinex-hacker-and-wife-plead-guilty-money-laundering-conspiracy-involving-billions (Accessed 20 April 2024).

14. “Two Foreign Nationals Arrested for Laundering at Least $73M Through Shell Companies Tied to Cryptocurrency Investment Scams” available at: https://www.secretservice.gov/newsroom/releases/2024/05/two-foreign-nationals-arrested-laundering-least-73m-through-shell (Accessed 20 April 2024).

15. “Massive blow to criminal Dark Web activities after globally coordinated operation” available at: https://www.europol.europa.eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation (Accessed 20 April 2024).

Стаття надійшла до друку 23 квітня 2024 року