УДК: 343.98

https://doi.org/10.52058/2786-6300-2023-7(13)-409-420

Самойленко Олена Анатоліївна головний науковий співробітник відділу дослідження проблем протидії кіберзлочинам та загрозам інформаційної безпеці Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України, доктор юридичних наук, професор кафедри криміналістики, Національний університет «Одеська юридична академія», пл. Солом'янська, 1,м. Київ, 03035, https://orcid.org/0000-0002-8925-4116

Тітуніна Катерина Вікторівна головний науковий співробітник відділу дослідження проблем протидії кіберзлочинам та загрозам інформаційної безпеці, Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України, кандидат юридичних наук, пл. Солом'янська, 1, м. Київ, 03035, https://orcid.org/0000-0003-2800-345X

ТИПОВІ КРИМІНАЛІСТИЧНІ ЗАСОБИ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ КРИПТОВАЛЮТ

Анотація Статтю присвячено проблемам вчинення та розслідування кримінальних правопорушень, пов'язаних із використанням криптовалют. Кінцева мета дослідження цих проблем полягає у визначенні типових криміналістичних засобів розслідування таких кримінальних правопорушень. Констатується, що для визначення інструментів, що використовуються правоохоронними органами підчас розкриття та розслідування таких правопорушень важливими є безпосередньо ознаки властиві криптовалютам та типові тактичні завдання розслідування кримінальних правопорушень, вчинених із використанням криптовалюти.

Криміналістичні засоби розслідування розглядаються базуючись на двох основних тактичних завданнях розслідування, зокрема: 1) блокування операцій з продажу криптовалюти певною особою; 2) ідентифікація особи або групи осіб, які здійснюють криптовалютні операції з незаконною метою.

Констатується, що перше тактичне завдання розслідування можна розв'язати теоретично двома методами: 1) блокування зв'язку між учасниками мережі, що перешкоджає відправці транзакцій повним вузлам, а також поширенню блоків через них; 2) блокування бірж криптовалют. Названі методи не можуть бути реалізовані в Україні а також багатьох інших державах

через відсутність організаційних та правових передумов для блокування. Вироблення системи суб'єктів співробітництва з постачальниками послуг, що перебувають на території іншої сторони (держави), щодо питань розкриття збережених комп'ютерних даних, та алгоритму дій правоохоронних органів з вищенаведеною метою якісно вплине на встановлення і закріплення криміналістично значущої інформації про факт вчинення конкретного кримінального правопорушення, пов'язаного із криптовалютою.

Розв'язання другого тактичного завдання розслідування вимагає від правоохоронних органів комбінування традиційних криміналістичних засобів розслідування злочинів, яке забезпечить процесуальне закріплення використання спеціального аналітичного програмного забезпечення, спрямованого на комплексний аналіз криптовалютних мереж. Такими типовими криміналістичними засобами розслідування кримінальних правопорушень, пов'язаних із використанням криптовалют, є негласні слідчі (розшукові) дії, зокрема: зняття інформації з транспортних телекомунікаційних мереж; зняття інформації з електронних інформаційних систем або її частини; обстеження публічно недоступних місць, житла чи іншого володіння особи; контроль за вчиненням злочину.

Ключові слова: блокування, злочин, інструмент, криміналістичний засіб, кримінальне правопорушення, криптовалюта, транзакція.

Samoilenko Olena Anatolyivna chief researcher of Research Department for Combating Cybercrime and Information Security Threats Interdepartmental Research Center for Combating Organized Crime under the National Security and Defense Council of Ukraine, Doctor of Laws, Professor, pl. Solomyanska, 1, Kyiv, 03035, https://orcid.org/0000-0002-8925-4116

Titunina Kateryna Viktorivna chief researcher of Research Department for Combating Cybercrime and Information Security Threats Interdepartmental Research Center for Combating Organized Crime under the National Security and Defense Council of Ukraine, Ph.D of Laws pl. Solomyanska, 1, Kyiv, 03035, https://orcid.org/0000-0003-2800-345X

TYPICAL FORENSIC MEANS OF INVESTIGATING CRIMINAL OFFENSES RELATED TO THE USE OF CRYPTOCURRENCIES

Abstract. The article is devoted to the problems of committing and investigating criminal offenses related to the use of cryptocurrencies. The ultimate goal of researching these problems is to identify typical forensic means of investigating such criminal offenses. It is stated that for the determination of the

tools used by law enforcement agencies during the disclosure and investigation of such offenses, the characteristics specific to cryptocurrencies and the typical tactical tasks of investigating criminal offenses committed with the use of cryptocurrency are important.

Forensic means of investigation are considered based on two main tactical tasks of the investigation, in particular: 1) blocking transactions for the sale of cryptocurrency by a certain person; 2) identification of a person or a group of persons who carry out cryptocurrency operations with an illegal purpose.

It is noted that the first tactical task of the investigation can be solved theoretically by two methods: 1) blocking communication between network participants, which prevents the sending of transactions to full nodes, as well as the distribution of blocks through them; 2) blocking cryptocurrency exchanges. These methods cannot be implemented in Ukraine and many other countries due to the lack of organizational and legal prerequisites for blocking. The creation of a system of subjects of cooperation with service providers located in the territory of the other party (state) regarding the disclosure of stored computer data and the algorithm of actions of law enforcement agencies with the above purpose will qualitatively affect the establishment and consolidation of forensically significant information about the fact of committing a specific criminal offense related to cryptocurrency.

Solving the second tactical task of the investigation requires law enforcement agencies to combine traditional forensic means of investigating crimes, which will ensure the procedural consolidation of the use of special analytical software aimed at comprehensive analysis of cryptocurrency networks.

Such typical forensic means of investigation of criminal offenses related to the use of cryptocurrencies are covert investigative (search) actions, in particular: removal of information from transport telecommunication networks; removal of information from electronic information systems or part thereof; examination of publicly inaccessible places, housing or other property of a person; control over the commission of a crime.

Keywords: blocking, crime, tool, forensic tool, criminal offense, cryptocurrency, transaction.

Постановка проблеми. Поява технологій розподіленого зберігання даних блокчейн (BlockChain) та заснованих на таких технологіях криптовалютних платіжних систем безпосередньо зумовили зміни механізмів вчинення кримінальних правопорушень різних видів, зокрема легалізації злочинних доходів, корупційних злочинів, злочинів у сфері бігу наркотичних засобів, психотропних речовин та прекурсорів, у сфері охорони державної таємниці, кіберзлочинів тощо. Європол також звернув увагу на ризики використання продуктів технології блокчейн. У своєму звіті про загрози

організованої злочинності в Інтернеті він дійшов висновку, що тренди обігу криптовалюти мають широку популярність у кримінальній сфері [1]. Однак, оновились не тільки інструменту сучасних злочинців, наявність у відкритому доступі бази даних транзакцій у системі криптовалюти дає правоохоронцям також нові інструменти боротьби зі злочинністю – модернізуються криміналістичні засоби розслідування кримінальних правопорушень, пов'язаних із використанням криптовалют. [2].

Аналіз останніх досліджень і публікацій. У науковому дискурсі питання криптовалют в основному піднімались з позицій цивілістики, господарського та банківського права. І. Верес, М. Гребенюк, А. Горбунова, В. Іванюк, М. Карчевський, О. Кремінський, В. Кубай, О. Мельниченко, Д. Пашко, К. Черевко та багато інших науковців розглядали питання фінансово-правової сутності, правового статусу криптовалют, а також їх впливу в цілому на структуру та динаміку злочинності. Втім, в криміналістичній науці вчені зовсім не піднімають проблеми вчинення злочинів за допомогою криптовалют та розслідування таких злочинів.

Мета статті – визначити типові криміналістичні засоби розслідування кримінальних правопорушень, пов'язаних із використанням криптовалют.

Виклад основного матеріалу. З огляду на чинні норми законодавства України (Цивільний кодекс України, Закон України «Про Національний банк України», Декрет Кабінету Міністрів України «Про систему валютного регулювання і валютного контролю», Закон України «Про платіжні системи та переказ коштів в Україні», Закон України «Про інформацію» та інші) поняття «криптовалюта» залишається невизначеним, а операції з нею не мають чіткого правового режиму. В правовому полі йдеться лише про «віртуальні активи», в прийнятому 17 березня 2022 року Законі України «Про віртуальні активи» визнається, що віртуальний актив – це нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі [3]. У свою чергу, сам Закон України «Про віртуальні активи» досі не набув чинності, це відбудеться з дня набрання чинності закона України про внесення змін до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами. 13 березня 2022 р. Верховною Радою України було одержано лише Проєкт такого закону («Про внесення змін до Податкового кодексу України щодо оподаткування операцій з віртуальними активами») за № 7150 [4], який досі не прийнято.

Хоча Закон України «Про віртуальні активи» й називають основним регулятором криптовалют, але в ньому не має відповіді на питання чи тотожний віртуальний актив криптовалюті, як саме віртуальний актив співвідноситься з електронними грошима. Такої відповіді немає в жодному сьогодні діючому нормативному акті. До того ж в ч. 3 ст. 2 Закону визнається,

що дія Закону також не розповсюджується на правовідносини, пов'язані з обігом електронних грошей та цінних паперів.

У жовтні 2019 року Законом Україні «Про внесення змін до деяких законодавчих актів України щодо забезпечення ефективності інституційного механізму запобігання корупції» [5] законодавцем внесено зміни до пункту 6 статті 46 Закону України «Про запобігання корупції», де визначено, що декларуванню підлягають нематеріальні активи, що належать суб'єкту декларування або членам його сім'ї, у тому числі об'єкти інтелектуальної власності, що можуть бути оцінені в грошовому еквіваленті, криптовалюти. А з з прийняттям в Україні Закону «Про віртуальні активи», низка зарубіжних дослідників зауважили, що криптовавлюти в цьому сенсі будуть додатковим інструментом для корупціонерів, погіршаться корупційні проблеми держави [6]. Й дісно кількість чиновників, які задекларовують криптовалюти стала зростати. Так, у 2016 році їх було 25 осіб, то у 2021 році – 700 осіб. Вони задекларували 46351 монет біткоїн, що складає на сьогодні 2 мільярди 700 мільйонів доларів США [7]. Згідно даним Національного агентства з питань запобігання корупції [8] проведено 28 повних перевірок декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, у яких задекларовано відомості про криптовалюту. Суб'єктами декларування задекларовано криптовалюти за видами у наступній кількості: Bitcoin (Біткоїн, біткоін, BTC) – 9158,175814 од.; Ethereum (Etherium, ETH) – 5780,760058 од.; Ethereumclassic – 135 од.; Litecoin – 2306 од.; Dogecoin – 11820 од.; NEM – 15156 од.; Neo – 3160 од.; BitcoinCash – 5147 од.; BitcoinGold – 5147 од.; EOS – 1285 од.; Cardano – 3704 од.; Chainlink – 1355 од.; Firo – 1135 од.; Bitcoin SV – 5147 од.; Aelf – 3073 од.; Tron – 6993 од.; BitTorrent – 10471 од.; BitcoinToken – 9589 од.; Grin – 1053 од.; Ravencoin – 7293 од.; Zilliqa – 12930 од.; BitcoinZ – 45283 од.; Stellar (XLM) – 831300 од.; ZEC – 100 од.; Monero (XMR) – 381428 од.; Ripple – 20000 од.; Syntropy – 3160 од.; SwissBorg – 6,391 од.; Utrust – 2309 од.; USDT – 0,470702 од.; OneCoin – 1800 одиниць. При цьому за результатами повної перевірки декларацій у 22 поданих суб'єктами декларування в деклараціях виявлено недостовірні відомості про задекларовану криптовалюту. Під час повної перевірки декларацій 18 суб'єктів декларування не змогло довести походження грошей, витрачених на придбання криптовалюти. Під час повної перевірки декларацій 23 суб'єкта декларування не змогли надати підтверджуючої інформації про розміщення задекларованої криптовалюти в блокчейні за її індивідуально визначеною публічною адресою (адресою гаманця). Крім того, суб'єкти, щодо яких проведено моніторинг способу життя, задекларували криптовалюту за видами у наступній кількості: Біткойн Кеш - 89,347 од.; Біткоін – 112 од.; Монеро – 500 одиниць. Вищезазначені

суб'єкти не надали підтверджувальну інформацію щодо задекларованої криптовалюти.

З точки зору практичних міркувань, в сенсі цієї роботи та відповідно практично-прикладної функції криміналістики, дуже важливою є концепція віртуальної валюти. Віртуальні валюти – це різновид цифрової валюти, яка зазвичай контролюється її творцями та використовується та приймається членами певної віртуальної спільноти, наприклад у комп'ютерній грі. Усі віртуальні валюти є цифровими, але не всі цифрові валюти є віртуальними – вони існують за межами певної віртуальної спільноти, як-от електронні гроші на банківських рахунках. Концептуальний обсяг терміну «віртуальний актив» охоплює набагато ширше коло об'єктів цифрового світу, ніж самі віртуальні валюти, що робиться законодавцем фактично з метою збереження технологої нейтральності і охоплення цим визначенням (обсяг регулювання) найширшого спектра елементів кіберпростору, можливо з враховуванням можливих в майбутньому нових технологічних рішень у сфері обігу віртуальної валюти. На сьогодні одним із основних поділів віртуальних валют є поділ на конвертовані віртуальні валюти (в американському законодавстві відомі як CVC - convertible virtual currency) і неконвертовані, такі як Project Entropia Dollars, QQ Coins, WoW Gold. Також часто розрізняють централізовані віртуальні валюти (наприклад, WoW Gold або e-Gold) і децентралізовані (без центральної точки адміністрування, наприклад, BTC або ETH).

Для розуміння інструментів, що використовуються правоохоронними органами підчас розкриття та розслідування злочинів, пов'язаних із використанням криптовалют, важливою є така ознака криптовалюти як легкість її обігу. Важко уявити навіть тимчасове призупинення роботи децентралізованої мережної структури, крім всесвітнього збою Інтернету. Мережа, що базується на тисячах повних вузлів, розкиданих по всьому світу, із записом усього блокчейну та можливістю перевірки транзакцій, пропонує порівняно з банківською системою більш вищий рівень безпеки зберігання даних. При цьому такий переказ є легким для користувача. Мільйон доларів готівкою складно перевезти на інший кінець світу або надіслати через традиційний банківський канал не привертаючи уваги різних служб, для криптовалюти достатньо надіслати закритий ключ (64 символи).

В процесі розслідування злочинів, пов'язаних із використанням криптовалют, часто виникає необхідність розв'язати два тактичних завдання.

Перше тактичне завдання – це блокування операцій з продажу криптовалюти певною особою. Проблемою його розв'язання є саме легкість обігу криптовалюти. Вважається що таке блокування можна здійснити двома методами: 1) блокування зв'язку між учасниками мережі, що перешкоджає

відправці транзакцій повним вузлам, а також поширенню блоків через них; 2) блокування бірж криптовалют, що перешкоджає продажу або обміну накопичених коштів на фіатні валюти (прийняті для розрахунків в державах).

Перший метод був би найефективнішим. Адже якщо відключити майнерів від отримання інформації про зроблені перекази, вони не будуть включені в блок. Однак, без додаткової технологічної системи – Great Firewall, яку має лише Китай, – реалізувати це не можливо. Китай вже блокував роботу всієї мережі Bitcoin на своєї території.

Другий спосіб технологічно набагато простіший у виконанні – він базується на модифікації DNS (системи доменних імен), блокуванні IP-адрес серверів, на яких розміщені такі веб-сайти, або блокуванні URL-адрес, і, отже, запобігання доступу користувачів. Таке блокування можуть здійснювати суб'єкти, що надають послуги доступу до мережі Інтернет (оператори и провайдери). Але тут виникає ряд організаційних та правових проблем через те, що ці суб'єкти завжди знаходяться під юрисдикцією іншої держави.

На Міжнародному рівні механізм протидії в цілому кіберзлочинам, визначений Конвенцією про кіберлочинність (Будапештська конвенція). Особливо важливим документом в цьому сенсі є Другий додатковий протокол до Конвенції, який станом на 1 червня підписали лише 30 держав. Він спрямований на посилення співпраці та розкриття електронних доказів. Україна приєдналась до Другого протоколу в грудні 2022 року, втім він ще залишається нератифікованим. Аналіз його змісту вказує на те, що на міжнародному рівні протидії кіберзлочинності з'явився новий дієвий інструмент для розширеної співпраці, документування та отримання електронних доказів [9]. В ст.ст 6, 7 Додатку до Конвенції йдеться про пряме співробітництво з постачальниками послуг та суб'єктами, що перебувають на території іншої сторони, а також між органами з питань розкриття збережених комп'ютерних даних. Він саме скерований на оперативне використання даних й теоретично його можна було б використати з метою блокування операцій з криптовалютою.

Сьогодні в Україні існує багато проблемних питань, що унеможливлюють блокування операцій з продажу криптовалюти певною особою. Так, згідно зі ст. 545 КПК України центральними органами міжнародного співробітництва в Україні є Офіс Генерального прокурора, Національне антикорупційне бюро України та Міністерство юстиції. Згідно зі ст. 35 Конвенції про кіберзлочинність вимагається створення цілодобової мережі (24/7) для надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення. Така

допомога включає сприяння або, якщо це дозволяється її внутрішньодержавним законодавством і практикою, пряме: надання технічних порад; збереження даних відповідно до ст.ст. 29 і 30; збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних. Наразі таке реагування на запити здійснює Департамент кіберполіції Національної поліції України по каналах Національної Цілодобової мережі контактних пунктів. Сьогодні більшість запитів надходять саме каналами Національного контактного пункту, вони й стосуються спілкування з операторами та провайдерами телекомунікацій, що знаходяться за межами України, як правило, це про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання, так як ця інформація здебільшого має суто технічний характер та є первинною інформацією при проведенні перевірки за будь-яким фактом учинення кримінального правопорушення. Проте, відповідно до чинного законодавства, виконання запитів від органів досудового розслідування інших держав не входять до його компетенції [10] й вони не є центральним органом міжнародного співробітництва. В Україні також згідно зі ст. 121 Закону України «Про електронні комунікації», доступ до інформації про споживача, факти надання електронних комунікаційних послуг, у тому числі до даних, що обробляються з метою передачі такої інформації в електронних комунікаційних мережах, здійснюється виключно на підставі рішення суду, слідчого судді у випадках та порядку, передбачених законом [11]. Тож, для реалізації положень конвенції в частині виконання таких запитів необхідно на законодавчому рівні визнати відповідні повноваження хоча б за Департаментом кіберполіції НП України або Службою безпеки України, можливо іншими суб'єктами, що протидіють злочинам, вчиненим із використанням криптовалюти.

Друге тактичне завдання розслідування визначеного виду злочинів – ідентифікація особи або групи осіб, які здійснюють криптовалютні операції з незаконною метою. Транзакції в мережах технології «блокчейн» анонімні по відношенню до користувачів як осіб, але не анонімні по відношенню до самих транзакцій. Тому мережі технології «блокчейн» з безліччю транзакцій можуть бути піддані цілісному та взаємопов'язаному аналізу, що дає можливість боротьбі з кримінальними правопорушеннями, пов'язаними із корупцією. Для виявлення та відслідковуваня незаконної діяльності у мережах технології «блокчейн використовуються спеціальні знання та відповідно спеціальне програмне забезпечення (наприклад, «Crystal» «Chainalysis», «CipherTrace», «CryptoFinance»,«BitcoinAbuseDatabas», «Walletexplorer.com», «Graphsense.info» [12]), яке безпосередньо здатне: виявити злочинну діяльність на блокчейні (дозволяє визначити, чи пов'язаний

гаманець із системами, які активно використовуються в незаконній діяльності, наприклад, у прихованій мережі, у системах «маскування» походження коштів тощо); виявити та задокументувати докази угод підозрюваного (вказавши всі адреси гаманців, які пов'язані з підозрюваним, можна визначити будь-які спроби приховати джерело або місце призначення незаконних коштів); прискорити розслідування (дозволяє автоматизовано відстежити найбільш підозрілих учасників мережі, зменшивши час на аналіз транзакцій вручну та запобігання невизначеності у постановки завдань) тощо. Використання ПЗ, здатного проводити комплексний та систематизований аналіз у криптовалютній мережі надає можливість ефективно аналізувати взаємозв'язки між транзакціями, встановлювати в решті-решт схеми потоків кримінальних фінансів.

Процедура застосування технічних засобів під час документування кримінальних правопорушень, вчинених із використанням криптовалюти, повинна бути такою, щоб матеріали такого застосування можна було долучати до матеріалів кримінального провадження. Отримані з використанням спеціального програмного засобу матеріали мають незаперечні переваги – документальність і високу інформативність. Вони надають можливість переглянути та доказати факт вчинення правопорушення. Це одне з найважливіших переваг, оскільки отримувати оперативну інформацію про вчинення кримінального правопорушення можна з різних джерел. Водночас тільки достовірність створених технічно матеріалів можна перевірити за допомогою експертизи.

Головний аспект використання таких матеріалів знаходиться в процесуальній площині. Негласні слідчі (розшукові) дії, що реалізуються у сфері інформаційно-телекомунікаційних технологій, зокрема:

- зняття інформації з транспортних телекомунікаційних мереж,
- зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи не пов'язаний з подоланням системи логічного захисту;
- зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача;
- обстеження публічно недоступних місць, житла чи іншого володіння особи;
- контроль за вчиненням злочину, – забезпечуть процесуальний момент фіксації інформації про операції з криптовалютами. В цьому сенсі суть таких дій повинна відображати дві сторони діяльності їх виконавців: зовнішнє сприйняття інформації (візуальний огляд та опис інформації, розміщеної на веб-ресурсі) та технологічний, пов'язаний із застосуванням можливостей спеціального програмного забезпечення для фіксації даних відповідних спеціалістом.

Матеріали, отримані в результаті використання спеціального ПЗ, можуть залучатися до процесу доказування, по-перше, як матеріали, що супроводжують (або доповнюють) показання осіб, по-друге, як документи, що не мають самостійного процесуального значення, але були отримані як додатки до протоколів слідчих (розшукових) та негасних слідчих (розшукових) дій. Істинність таких матеріалів, отриманих за допомогою технічних засобів, може бути додатково підтверджена результатами комп'ютерно-технічної експертизи.

Висновки. Отже, використання криптовалюти при вчиненні кримінальних правопорушень вимагає від правоохоронних органів таке комбінування традиційних криміналістичних засобів розслідування злочинів (зокрема негласних слідчих (розшукових) дій), яке забезпечить процесуальне закріплення використання спеціального аналітичного програмного забезпечення, спрямованого на комплексний аналіз криптовалютних мереж. Як й в більшості інших держав в Україні необхідним є створення організаційних та правових передумов для здійснення при необхідності блокування бірж криптовалют. Вироблення системи суб'єктів співробітництва з постачальниками послуг, що перебувають на території іншої сторони (держави), щодо питань розкриття збережених комп'ютерних даних, алгоритму дій правоохоронних органів з вищенаведеною метою якісно вплине на встановлення і закріплення криміналістично значущої інформації про факт вчинення конкретного кримінального правопорушення, пов'язаного із криптовалютою.

Література:

1. Internet organized crime threat assessment (IOCTA). Strategic, policy and tactical updates on the fight against cybercrimehttps. URL: https://www.europol.europa.eu/iocta-report.

2. Site «Just» Site «Just». Аналітика. URL: https://justtalk.com.ua/post/kriptovalyuti-ta-tehnologii-blockchain-innovatsii-u-protidii-koruptsii

3. Про віртуальні активи: Закон України № 2074-IX від 17 березня 2022 р. URL:https://zakon.rada.gov.ua/laws/show/2074-20#Text

4. Про внесення змін до Податкового кодексу України щодо оподаткування операцій з віртуальними активами: Проєкт Закону №7150. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/39211

5. Про внесення змін до деяких законодавчих актів України щодо забезпечення ефективності інституційного механізму запобігання корупції: Закон України // Відомості Верховної Ради (ВВР). 2019. № 47. Ст.311.

6. Braw E. Ukraine Wants to Be Cryptocurrency Central. Foreign Poicy. 02.06.2021. URL: https://foreignpolicy.com/2021/06/02/ukraine-wants-to-be-cryptocurrency-central/

7. Черево К.О. Криптовалюта як предмет відмивання доходів, одержаних злочинним шляхом. Протидія корупції: правове регулювання і практичний досвід : зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 3 груд. 2021 р.). ХНУВС. 2021. С. 72-75

8. Національного агентства з питань запобігання корупції. Ліст НАЗК №461-04/18817-22 від 02.09.2022

9. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence [Strasbourg, 12.V.2022]. URL: https://rm.coe.int/1680a49dab.

10. Про затвердження Положення про Департамент кіберполіції НП України: Наказ Національної поліції України № 85 від 10 листопада 2015 р. *Офіційний матеріал Департаменту Документального забезпечення Національної поліції України.* Відомчий документ.

11. Про електронні комунікації: Закон України № 1089-IX від 16.12.2020 р. (Із змінами). URL: https://zakon.rada.gov.ua/ laws/show/1089-20#n2246

12. Petrova M. M. (2017). Integration of the information processes. Automation and unification of the judicial system, Simon Kuznets Kharkiv National University of Economics, *«Economics of Development»*, ISSN 1683-1942. 2017. No 2 (82), p. 50-59

References:

1. Sait Europol. [Site Europol]. Internet organized crime threat assessment (IOCTA). Strategic, policy and tactical updates on the fight against cybercrimehttps. *europol.europa.eu/iocta-report*. Retrieved from https://www.europol.europa.eu/iocta-report.

2. Sait yzdatelskoi hrypu «Just». [Site «Just»]. *justtalk.com.ua/post/kriptovalyuti-ta-tehnologii-blockchain-innovatsii-u-protidii-koruptsii*. Retrieved from https://justtalk.com.ua/post/kriptovalyuti-ta-tehnologii-blockchain-innovatsii-u-protidii-koruptsii

3. Zakon Ukrainy «Pro vertualni aktyvy» [The Law of Ukraine « About virtual assets»]. (n.d.). *zakon.rada.gov.ua/laws/show/2074-20#Text*. Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20#Text

4. Proiekt Zakonu №7150 «Pro vnesennia zmin do Podatkovoho kodeksu Ukrainy shchodo opodatkuvannia operatsii z virtualnymy aktyvamy» [Draft Law No. 7150. On Amendments to the Tax Code of Ukraine on Taxation of Transactions with Virtual Assets (n.d.). itd.rada.gov.ua/billInfo/Bills/Card/39211. Retrieved from https://itd.rada.gov.ua/billInfo/Bills/Card/39211

5. Zakon Ukrainy Pro vnesennia zmin do deiakykh zakonodavchykh aktiv Ukrainy shchodo zabezpechennia efektyvnosti instytutsiinoho mekhanizmu zapobihannia koruptsii: pryiniatyi 2 zhovtnia 2019 roku № 140-IX [Law of Ukraine On making changes to some legislative acts of Ukraine on ensuring the effectiveness of the institutional mechanism for the prevention of corruption from zhovtnia 2 2019, № 140-IX]. (2019, Hovtnia 2). Vidomosti Verkhovnoi Rady (VVR) – Verkhovna Rada information, 47, St 311. [in Ukrainian].

6. Braw E. (2021). Ukraine Wants to Be Cryptocurrency Central. Foreign Poicy, 02.06.2021. Retrieved from https://foreignpolicy.com/2021/06/02/ukraine-wants-to-be-cryptocurrency-central/

7. Cherevo, K.O. (2021) Kryptovaliuta yak predmet vidmyvannia dokhodiv, oderzhanykh zlochynnym shliakhom [Cryptocurrency as a subject for laundering proceeds of crime]. Proceedings from KhNUVS '21: Mizhnarodna naukovo-praktychna konferentsiia «Protydiia koruptsii: pravove rehuliuvannia i praktychnyi dosvid» – The International Scientific and Practical Conference « Anti-corruption: legal regulation and practical experience». (pp. 72-75). Kharkiv : KhNUVS [in Ukrainian].

8. Natsionalnoho ahentstva z pytan zapobihannia koruptsii. List NAZK №461-04/18817-22 (2022) – [National agency for the prevention of corruption. Letter of NAZK].[in Ukrainian].

9. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence [Strasbourg, 12.V.2022]. *rm.coe.int/1680a49dab*. Retrieved from https://rm.coe.int/1680a49dab.

10. Nakaz Natsionalnoi politsii Ukrainy Pro zatverdzhennia Polozhennia pro Departament kiberpolitsii NP Ukrainy: pryiniatyi 10 lystopad 2015 roku [Order of the National Police of Ukraine Approving the Regulation on the Cyber Police Department of the National Police of Ukraine from lystopad 2015. (2015, lystopad 10). Ofitsiinyi material Departamentu Dokumentalnoho zabezpechennia Natsionalnoi politsii Ukrainy. Vidomchyi document – Official material of the Department of Documentary Support of the National Police of Ukraine. Official document. [in Ukrainian].

11. Zakon Ukrainy «Pro elektronni komunikatsii » [The Law of Ukraine «About electronic communications»]. (n.d.). *zakon.rada.gov.ua/ laws/show/1089-20#n2246*. Retrieved from https://zakon.rada.gov.ua/ laws/show/1089-20#n2246

12. Petrova, M. M. (2017). Integration of the information processes. Automation and unification of the judicial system, Simon Kuznets Kharkiv National University of Economics, «Economics of Development»,. (Vols. 2), (pp. 50-59). Kharkiv: Kharkiv National University of Economics [in Ukrainian]. p. 50-59