УДК 342.951

КАЛАЙДА Ю.П., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-1408-2145.

МОЖЛИВОСТІ БЛОКЧЕЙН-ТЕХНОЛОГІЙ У РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ В КІБЕРПРОСТОРІ

Анотація. *Актуалізовано загрозливі тенденції розвитку цифрової економіки. Узагальнено роль, місце та значення криптовалют та технології блокчейн у сучасному світі. Зроблено акцент на проблемних питаннях використання криптовалют як платіжного засобу у мережі Інтернет, який використовується у протиправній діяльності. Розглянуто особливості проведення трансакцій з криптовалютами, які здійснює криміналітет для фінансування протиправної діяльності. Деталізовано напрями правоохоронної діяльності з метою запобігання та технологічного блокування незаконних операцій з криптовалютами. Висвітлено здобутки та досягнення використання програмного забезпечення "Crystal". Окреслено проблемні питання накладання арешту та здійснення конфіскації криптовалютних засобів, які використовувалися у злочинних цілях. Визначено засади удосконалення правоохоронної діяльності у сфері розслідування кримінальних правопорушень, скоєних в кіберпросторі.*

Ключові слова: *блокчейн, цифрові технології, цифровізація, криптовалюта, злочинність, фінансові активи, правоохоронна діяльність, міжнародно-правове регулювання криптовалюти.*

Summary. *The threatening trends in the digital economy have been reviewed. The role, place and significance of cryptocurrencies and blockchain technologies in the modern world are generalized. Emphasis is placed on the problematic issues of using cryptocurrencies as a means of payment on the Internet, which is used in illegal activities. The peculiarities of conducting transactions with cryptocurrencies carried out by criminals to finance illegal activities are considered. The directions of law enforcement activity aimed at prevention and technological blockade of illegal operations with cryptocurrencies are detailed. The achievements and accomplishments of the use of "Crystal" software are highlighted. The problematic issues of seizing and confiscating cryptocurrency funds used for criminal purposes are outlined. The principles of improving law enforcement activities in the field of investigation of criminal offenses committed in the cyber space are determined.*

Keywords: *blockchain, digital technologies, digitalization, cryptocurrency, crime, financial assets, law enforcement, international legal regulation of cryptocurrencies.*

Аннотация. *Актуализированы угрожающие тенденции развития цифровой экономики. Обобщены роль, место и значение криптовалют и технологии блокчейн в современном мире. Акцентировано внимание на проблемных вопросах использования криптовалют в качестве платежного средства в сети Интернет, используемого в противоправной деятельности. Рассмотрены особенности проведения трансакций с криптовалютами, осуществляемых криминалитетом для финансирования противоправной деятельности. Детализированы направления правоохранительной деятельности для предотвращения и технологического блокирования незаконных операций с криптовалютами. Освещены результаты и достижения использования программного обеспечения "Crystal". Определены проблемные вопросы ареста и конфискации криптовалютных средств, используемых в преступных целях. Определены основы усовершенствования правоохранительной деятельности в сфере расследования уголовных правонарушений, совершенных в киберпространстве.*

Ключевые слова: *блокчейн, цифровые технологии, цифровизация, криптовалюта, преступность, финансовые активы, правоохранительная деятельность, международно-правовое регулирование криптовалют.*

Постановка проблеми. Розвиток цифрової економіки не тільки відкриває нові можливості для суспільства та держави, але й озброює злочинців новими методами здійснення правопорушень, створює додаткові загрози для численних сфер громадського та суспільного життя. Інформатизація кредитно-фінансової системи зумовила появу нових сучасних механізмів фінансових розрахунків. При цьому технічні засоби та методи, що використовуються у фінансовій діяльності постійно удосконалюються. В умовах поширення пандемії у світових масштабах був спровокований вимушений перехід на дистанційний режим роботи, що призвело до збільшення кількості кримінальних правопорушень, вчинених з використанням передових інформаційних технологій. Шахрайства з платіжними картками, крадіжки грошей із банківських рахунків, розповсюдження комп'ютерних вірусів, викрадення хакерами персональних даних громадян, онлайн-торгівля наркотиками, поширення протиправного контенту – це лише невелика частина злочинів, які мають розслідувати та припиняти правоохоронні органи в сучасних умовах. Разом із динамічним розвитком інформаційних технологій та прагненням держави до суцільної цифрової трансформації усіх сфер суспільного життя, цифровий прогрес зумовлює появу нових та вдосконалення існуючих інструментів для здійснення кримінальних правопорушень.

Таким чином, тотальна цифровізація суспільства має зворотній бік, негативним проявом якого є поява нових кримінальних ризиків. Як свідчить статистика, різноманітні злочини, які вчинюються з використанням мережі Інтернет та інших інформаційних технологій, мають тенденцію до зростання. У зв'язку із появою нових форм суспільних відносин, які проникають у віртуальне середовище, актуальною та витребуваною технологією для передачі інформації у зашифрованому вигляді стала саме блокчейн технологія, на основі якої функціонує система обігу криптовалют. Свідченням того, що фінансові технології вийшли на світовому ринку на якісно новий рівень, є широке розповсюдження криптовалюти (віртуальної валюти), яка працює на основі децентралізованої системи блокчейн. Криптовалюти, які опанували світ, змінили уявлення не тільки про умови ведення бізнесу, але й приватних фінансів. Криптовалюта набирає популярності завдяки можливості розрахунку у віртуальному просторі, оскільки не потребується їх реальний вираз у вигляді грошових коштів, адже для таких розрахунків використовується лише цифровий ключ, захищений криптографічним кодом, що надійно захищає криптовалютні трансакції анонімного характеру. Принцип функціонування блокчейн технології зводиться до того, що усі списки операцій з криптовалютою об'єднуються у блоки, а блоки, у свою чергу, у ланцюги. При формуванні ланцюгів блоків через мережеві з'єднання децентралізований сервер формує базу даних, яка керується автономно без єдиного центру. Блокчейн технологія використовує криптографію та цифрові підписи для засвідчення певної особи: трансакції відслідковуються до криптографічних ідентифікаційних даних, які теоретично анонімні, проте можуть бути закріплені за реальними даними певного користувача.

Таким чином, функція блокчейн технологій полягає у реєстрації кожної трансакції з криптовалютою. Будь-яка передача криптовалюти підтверджується у мережі внесенням трансакційного блоку з використанням процесу шифрування, що забезпечує необхідну конфіденційність та анонімність. Ця технологія передачі та зберігання даних стала об'єктом уваги злочинців. Йдеться саме про криптовалюту, яка не платіжним засобом у буквальному значенні, проте фактично стала сурогатом емісійних платіжних засобів. Схема роботи криптовалют не регулюється будь-якими державними органами або фінансовими установами, а операції, що відбуваються з криптовалютами не регламентовані міжнародним законодавством, а тому ідентифікувати їх як злочинні не

можна. Однак, при здійсненні протиправної діяльності у мережі Інтернет, криптовалюта виступає засобом скоєння злочину та використовується у якості платіжного засобу для придбання вогнепальної зброї, наркотиків, легалізації злочинних доходів, фінансування тероризму тощо. Злочинці, використовуючи криптовалюту, здійснюють чималі грошові перекази через мережу Інтернет. Таким чином вони ігнорують використання звичайних фінансових систем, спричиняючи масштабні економічні збитки та посягаючи на основи національної безпеки тієї чи іншої держави. Враховуючи викладене, актуальним та своєчасним є розгляд особливостей використання можливостей технології блокчейн у розслідуванні злочинів, вчинених в кібепросторі.

Результати аналізу наукових публікацій. Кримінологічні засади злочинної діяльності з використанням криптовалют та технології блокчейн розглядали у своїх наукових працях: Благута Р.І. та Мовчан А.В. [1], Гребенюк М.В. та Черняк А.М. [2], Казначеєва Д.В. та Дорош А.О. [3], Клименко О.А. та Гуцалюк М.В. [4] та інші фахівці. Проте питання висвітлення кращих практик та методології розслідування злочинів, скоєних в Інтернет просторі за допомогою технології блокчейн, не було предметом окремого аналізу, що посилює актуальність обраного напрямку дослідження.

Метою статті є визначення особливостей інформаційно-аналітичного забезпечення правоохоронної діяльності з використанням блокчейн-технології, спрямованого на виявлення фактів та спроб використання криптовалют у протиправній діяльності в мережі Інтернет.

Виклад основного матеріалу. Уперше про ризики використання продуктів технології блокчейн повідомив Європол ще у 2015 році. У його звіті проаналізовано тренди обігу криптовалюти та використання нових фінансових інструментів у злочинних цілях. Було констатовано, що дедалі частіше криптовалюта використовується у мережі тіньового Інтернету – DarkNet (“Даркнет”) під час придбання вилучених з обігу речовин та наркотичних засобів. У 2018 році Європол прозвітував, що напрямки кримінального використання криптовалюти значно збільшилося, а криптовалюта переважно використовується як засіб розрахунків на тіньових Інтернет-ринках. У 2018 році ринок незаконної діяльності з Біткоїном складав близько $76 млрд. США. У 2019 – 2020 роках найбільша кількість злочинів, вченених з використанням криптовалют, стосувалася саме сфери мережевого шахрайства.

Популярність нового фінансового інструменту у кримінальному середовищі пояснюється тим, що на сьогодні не розроблені юридичні параметри криптовалюти та не встановлені кордони її безпечного обігу. Це обумовлено неповним розумінням вітчизняних та міжнародних експертів важливості дослідження криптовалюти у рамках ризик-орієнтованого підходу, коли одночасно робиться співвідношення економічних важелів та криміногенного потенціалу криптоінструментів. Відсутність комплексних досліджень кримінального використання криптовалюти негативно впливає результативність роботи у сфері запобігання та профілактики такої злочинної діяльності. Таким чином, своєчасним та практично значущим є кримінологічний аналіз криптозлочинності як самостійного об’єкта наукового пізнання та одночасно підсистеми кримінологічної моделі інтернет-злочинності.

Під криптозлочинністю слід розуміти сукупність системних протиправних дій, які здійснюються щодо криптовалюти або з її використанням. Оскільки це явище перебуває на стадії свого інституційного становлення, застосування цього поняття є досить умовним. Можна виділити 3 сектора криптозлочинності: незаконний продаж психоактивних речовин (наркотичних та психотропних засобів), інших заборонених товарів та послуг; відмивання злочинних доходів з використанням криптовалюти; крадіжка криптовалюти

та інші злочини проти власності. В сучасних умовах за криптовалюту можна придбати широкий спектр нелегальних товарів та послуг. Віртуальні гроші використовуються у сферах: порно індустрії; незаконного обігу персональних даних; торгівлі підробленими документами. Іноді навіть оплачуються замовні вбивства. Проте, найбільш поширеним сегментом криптозлочинності залишається саме незаконний обіг наркотичних засобів та психотропних речовин (80 % від загального обсягу ринку нелегальних товарів).

На жаль, на сьогодні світова статистика кримінального обігу наркотиків, порнографії, заборонених послуг з використанням криптовалюти не ведеться, проте згідно із даними експертів само криптовалюта є засобом розрахунків у 95 % операцій. При цьому спостерігається принципово нові кримінологічні тренди розвитку DarkNet: поступова специфікація окремих кримінальних сервісів та покращення їх технологічних характеристик; поступова монополізація криптовалютного ринку тощо. Відбувається тренд розширення спектру використання криптовалют для удосконалення трансакцій.

Якщо раніше абсолютним монополістом на криптовалютному ринку був Біткоїн, то зараз все частіше застосовуються нові цифрові валюти з високим ступенем анонімності (ZCash, Dash, Monero). Про це вказує у своїх звітах Європол. Дійсно, криптовалютні операції є анонімними, оскільки адреси криптовалютних гаманців, як правило, не пов’язані з певною особою. Проте, сам ланцюг трансакцій, який пов’язаний з певним гаманцем, не є анонімним. За необхідності, певний ланцюг трансакцій може бути проаналізовано, в результаті чого існує доля ймовірності ідентифікувати певну особу, якій належить конкретний криптовалютний гаманець, за зв’язками з іншими адресами у ланцюгу. Водночас існують системи, які дозволяють зберегти криптовалютні трансакції конфіденційними. Наприклад, це мережева система “Blender”, яка доступна за адресою //blender.io. Ця система надає послугу приховування реальних адресатів криптовалютних гаманців, з яких були отримані криптовалютні платежі. Це досягається тим, що сума, яку необхідно “замаскувати”, поділяється на частини та надсилається на адреси криптовалютних гаманців, які були створені для клієнта та не пов’язані з основною адресою криптовалютного гаманця, де грошові кошти зберігалися спочатку. Ця схема має за мету заплутати сліди походження засобів та ввести в оману правоохоронців у випадку розслідування злочинів з криптовалютами та блокування будь-яких спроб визначити реальну особу клієнта. Система “Blender” має достатню кількість резерву криптовалютних засобів, що надає змогу клієнту отримати свої засоби з початку ланцюга блоків. Саме тому походження засобів не буде відображатися. Наприклад, мережева система “Blender” не зберігає інформацію про оброблені трансакції, оскільки уся історія трансакцій знищується без можливості її майбутнього відновлення після того, як усі криптовалютні засоби надіслані на цільові адресати криптовалютних гаманців.

По факту розвитку нелегального та злочинного криптобізнесу формується його направленість з одночасною спеціалізацією осіб, які залучаються до злочинних схем. Виділяються такі нові кримінальні професії, як: координатори (адміністратори одночасно декілька сервісів); “єксроу” (гаранти угод); “гровери” (особи, які вирощують або комплектують наркотичні засоби); “кладмени” (особи, які розміщають відповідні об’яви та рекламу); “дропи” (особи, які приймають товар або здійснюють переказ криптовалют). Основна проблема використання криптовалюти у злочинних цілях полягає у наявних технічних труднощах ідентифікації особи або групи осіб, які здійснюють криптовалютні операції протиправного характеру. Злочинна діяльність може бути направлена на: легалізацію грошових коштів, тобто приховування їхнього

походження; здійснення платежів з метою організації шахрайських схем, злому інформаційних систем; фінансування тероризму тощо.

Наприклад, новим та популярним засобом легалізації кримінальних доходів є їх відмивання через сайти азартних ігор. Саме через ці сервіси відмиваються майже ¾ усіх "брудних" віртуальних грошей. Згідно даних "Trend Micro" злочинці все частіше використовують ігрову валюту як засіб зберігання вартості криптовалют. Для цього придбається валюта найбільш популярних віртуальних ігор. Вона продається за криптовалюту, а потім на спеціальних сервісах відбувається її конвертація на гроші. Існують великі ризики використання криптовалюти під час фінансування тероризму. Для більшості терористичних організацій єдиним способом залишається фізичне транспортування готівкових коштів. Однак, з огляду на розширення практики використання криптовалют та розвитку інфраструктури трансакцій, віртуальна валюта у майбутньому дедалі частіше буде використовуватися для фінансування тероризму.

Ще одну групу злочинів, які вчиняються з використанням криптовалюти, складають злочини проти власності, коли криптовалюта є об'єктом посягання. Особи, які викрадають криптовалюту, використовують фейкові (підробні) електронні гаманці. Потерплі, придбаючи товар або послуги на популярних сервісах, перераховують гроші на фішингові гаманці, які мають інші адреси, через використання вірусних програм. Це може бути створення фішингових сайтів популярних ресурсів. Використання криптовалюти у шахрайський спосіб також практикують краудінвестиційні проекти. Розвиток нової моделі колективного інвестування призвело до появи шахрайських компаній, які збирають від потерпілих гроші у криптовалютах без наміру займатися підприємницькою діяльністю.

Загалом, під час розслідування злочинів з використанням криптовалют правоохоронним органам необхідно мати відомості про: умови, порядок обігу криптовалют, особливості здійснення трансакцій, специфіку функціонування криптовалютних бірж тощо. Успішне розслідування вказаної категорії злочинів також є можливим лише при наявності кваліфікованих спеціалістів ІТ-сфери (інформаційно-комунікаційних технологій). Розслідуючи злочини, які вчиняються з використанням криптовалюти, доцільно враховувати той факт, що ці злочини мають свої специфічні особливості. Проте існують складності щодо визначення належності певної Біткоїн-адреси. Тому співробітники правоохоронних органів шукають засоби прив'язати певну IP-адресу або адресу електронної пошти до конкретної особи.

Однак, якщо особа використовує декілька IP-адрес, проксі-сервери, то цей процес стає набагато складнішим. Також, враховуючи технічну специфіку та особливості проведення криптовалютних операцій, існування процедур можливого маскування походження криптовалютних активів, доцільним вбачається розвиток засобів дослідження слідоутворення, розробки алгоритму встановлення та закріплення криміналістично вагомих відомостей для цього типу злочинів. Для досягнення цього ефекту, доцільно провести гармонізацію права у цьому напрямку. Трансакції у мережах технології блокчейн анонімні по відношенню до користувачів, проте не є анонімними щодо самих трансакцій. Тому технології блокчейн з різноманітними трансакціями мають бути піддані ґрунтовному аналізу, що надає змогу ефективно протидіяти злочинам, пов'язаним із криптовалютами. Для проведення такого аналізу необхідно мати спеціальні знання та спеціальне програмне забезпечення.

Наприклад, таким програмним забезпеченням є "Crystal", яке належить голландському підприємству – розробнику "Bitfury Group". Це програмне забезпечення здатне виявляти та відслідковувати незаконну діяльність у мережах технології блокчейн,

а саме: виявляти злочинну та протиправну діяльність у системах блокчейну; надавати докази щодо укладених підозрілих угод на криптовалютних біржах, зазначаючи при цьому адреси гаманців, які пов'язані з підозрюваною особою; прискорювати процес розслідування кіберзлочинів (дозволяє автоматизовано відслідковувати найбільш підозрілих учасників мережі) тощо. Вказане підприємство пропонує своє програмне рішення, у першу чергу, для правоохоронних органів. Доцільно вказати, що "Crystal" не обмежує свої можливості тільки у напрямку аналізу криптовалютної мережі. Воно здатне знаходити та структуризувати інформацію про адреси та змістовність мережі з інших джерел, таких як форуми або інші інтернет–портали. Завдяки такому комплексному підходу "Crystal" може встановити не тільки адресу певного об'єкту, а також його реальне ім'я та інші реквізити. Це програмне забезпечення активно використовується як правоохоронними органами, так і фінансовими організаціями у США, ЄС та країнах Азії.

Прикладом успішної роботи цього програмного забезпечення є боротьба з вірусом "WannaCry", в результаті чого були відслідковані платежі від жертв вірусу та встановлено особу, яка вимагала платежі. Існують також й інші програмні забезпечення, наприклад, "Chainalysis", "CipherTrace", "CryptoFinance" тощо. В основному завдання та функції даних програмних засобів схожі, проте відрізняються між собою алгоритмом аналізу та порядком отримання даних. Враховуючи здобутий досвід протидії цих програм злочинній діяльності, а також той факт, що вказане програмне забезпечення здатне здійснювати комплексний аналіз у криптовалютній мережі, їх практичне впровадження у правоохоронну діяльність неможливо недооцінювати. Доцільно вказати, що у випадку розкриття злочину постає закономірне питання арешту та у подальшому конфіскації криптовалютних засобів.

Однак, для вирішення цього питання правоохоронці стикаються як з правовими, так і технічними труднощами. На даний момент не існує єдиного загальноприйнятого правового врегулювання цих питань, яке б передбачало порядок арешту або конфіскації криптовалюти. Таким чином, не зрозуміло як бути, коли постає питання про арешт або конфіскацію криптовалюти, якщо правоохоронцям не відомий приватний цифровий ключ криптовалютного гаманця правопорушника. Це можливо, якщо правопорушник пам'ятає та знає свій приватний цифровий ключ, але розголошувати його ніхто не має права примусити. Тому якщо слідству відомо, що конкретній особі належить криптовалютний гаманець, без сприяння самого правопорушника арешт або конфіскація не можливі з технічних причин. У випадку неможливості арешту або конфіскації криптовалютних засобів, адреси криптовалютних гаманців, котрі використовуються у незаконній діяльності, можливо вносити до "чорних" списків, як це робить Департамент казначейства США. З метою запровадження подальших санкцій доцільно було б створити "чорний" список криптовалютних гаманців користувачів.

Проте непоодинокі випадки, коли криптовалютний гаманець прив'язаний до певної криптовалютної біржі. Тоді є можливість звернутися із запитом до суб'єкта, який здійснює обслуговування конкретної криптовалютної біржової системи з вимогою надати дані або здійснити арешт чи конфіскацію, наприклад, здійснити переказ засобів правопорушника на інший, створений для арешту або конфіскації криптовалютний гаманець. Водночас не усі криптовалютні біржі публікують свою контактну інформацію, а також інформацію про свій правовий статус, що не дає можливості для такого звернення. Також не завжди визначена юрисдикція таких підприємств. У результаті, якщо правопорушник надає сприяння або іншим способом можливо дізнатися про приватний цифровий ключ його криптовалютного гаманця, найбільш

оптимальним є переказ злочинних криптовалютних засобів на інший гаманець з метою подальшого арешту або конфіскації цих активів, оскільки залишати їх на поточному криптовалютному гаманці не можна. Інакше, криптовалютні активи можуть бути переказані на інші криптовалютні гаманці без відома правоохоронних органів.

Масштабне використання криптовалют у незаконній діяльності – це комплексна міжнародна проблема світової спільноти, а не однієї держави, оскільки криптовалютні операції здійснюються завдяки глобальної мережі Інтернет, яка не має територіальних та юрисдикційних кордонів. Проте, розуміючи ризики та загрози у вказаному сегменті, деякі держави світу активізують свої зусилля за напрямком протидії злочинному використанню криптовалют. Так, у 2021 році Міністерство юстиції США створило національну команду з захисту криптовалют (NCET) з метою проведення складних розслідувань і судового переслідування злочинних зловживань з криптовалютою. До складу команди увійдуть фахівці з декількох секторів Мін'юсту США – відділу з боротьби з відмиванням грошей і поверненням активів, а також відділу комп'ютерних злочинів та інтелектуальної власності. Основна мета та завдання діяльності цієї команди – зміцнити здатність протидіяти структурам, які процвітають і отримують прибуток завдяки зловживанням із криптовалютними платформами. Ця група має не тільки розслідувати складні фінансові злочини, а й відігравати допоміжну роль під час міжнародних та федеральних розслідувань, а також під час розслідувань на рівні штатів [5]. Також у 2021 році США вперше запроваджено санкції проти платформи для обміну криптовалюти, яка, як вважається, сприяла проведенню фінансових транзакцій осіб, причетних до програм-вимагачів. Казначейство США запровадило санкції проти чесько-російської криптовалютної біржі SUEX з реєстрацією в Москві та Празі, яка сприяла проведенню фінансових транзакцій осіб, причетних до програм-вимагачів. SUEX полегшувала транзакції, пов'язані з незаконними доходами. Аналіз відомих транзакцій SUEX демонструє, що понад 40 % транзакцій SUEX пов'язано з незаконними суб'єктами. Біржі віртуальних валют, такі як SUEX, мають вирішальне значення для прибутковості атак програм-вимагачів, які допомагають фінансувати діяльність кіберзлочинців. На переконання міністра фінансів США Джанет Єллен, програми-вимагачі та кібератаки заподіюють значну шкоду малому та великому бізнесу і становлять загрозу економіці країни.

На жаль, світовою спільнотою все ще не схвалено єдиного міжнародно-правового механізму, відсутність якого призводить до проблем визначення юрисдикцій впливу, наприклад, мережевих криптовалютних обмінних або біржових систем. Мережеві криптовалютні обмінні або біржові системи, а також інші системи, які надають будь-які криптовалютні послуги, які не афішують на своїх сайтах юридичну інформацію, наприклад, назву, реєстраційний номер підприємства, контактну інформацію тощо – це системи, які переважно здійснюють свою діяльність незаконно, оскільки приховують юридичну інформацію про свою діяльність, або взагалі здійснюють свою господарську діяльність без реєстрації. Це певним чином, ускладнює направлення запитів від правоохоронних органів до таких організацій. Можливо, такі не добропорядні системи доцільно блокувати або вносити їх у спеціальні "чорні" списки. Завдяки існуванню різноманітних аналітичних програм, які здатні проводити комплексні аналізи криптовалютних мереж, збільшуються можливості розкриття кримінальних правопорушень, які вчиняються з використанням криптовалюти.

Тому той факт, що адреси криптовалютних гаманців не пов'язані з конкретними особами не означає, що злочини, у скоєнні яких використовуються криптовалюти не розкриваються. Навпаки, сучасне програмне забезпечення сприятиме розкриттю

правоохоронцями не тільки фактів злочинної діяльності, але й дозволяє ідентифікувати не тільки особу правопорушника, але й відслідкувати маршрути потоків незаконних криптовалютних засобів. Проте потребує прискорення розробка міжнародно-правових механізмів інституту арешту та конфіскації незаконно отриманих криптовалютних засобів. Сучасні тенденції переконливо свідчать про те, що трансакції в криптовалютних мережах не є абсолютно анонімними, та можуть перебувати у фокусі уваги правоохоронних органів, зокрема шляхом організації проведення комплексного аналізу завдяки спеціальному програмному забезпеченню та іншим методам верифікації.

Висновки.

Технологія блокчейн, на основі якої функціонує криптовалютна індустрія має такі переваги: 1) стабільність; 2) безпечність; 3) прозорість роботи з даними; 4) транскордонний характер операцій з обміну даними. На цьому фоні основний пріоритет під час використання криптовалюти у злочинній діяльності – це відсутність прив'язки особи до певного криптовалютного гаманця та збільшення кількості кібератак з використання програм-вимагачів. Одним із найбільш популярних засобів обігу криптовалюти у злочинних цілях є функціонування криптовалютних бірж. У мережі Інтернет представлено чимало криптовалютних обмінних систем з невизначеною юрисдикцією. Внаслідок цього існує вірогідність, що ці сервіси можуть використовуватися у злочинній діяльності. Доцільно вказати, що досить активно криптовалюти як розрахункові засоби використовуються у мережі DarkNet, у якій дані передаються у зашифрованому вигляді. Також функціонує чимало площадок–сайтів, на яких здійснюється незаконна діяльність. Наприклад, тільки у 2019 році у прихованій мережі функціонувало понад 2,5 тис. магазинів наркотичних та психотропних речовин, у яких розрахунки відбувалися за допомогою криптовалюти.

Тому важливим напрямом протидії такому явищу залишається використання сучасного програмного забезпечення у правоохоронній діяльності. З метою ефективності розкриття злочинів, що вчинюються з використанням криптовалют, доцільним вбачається: прискорити схвалення правових засад, які мають врегулювати криптовалюти та розробку методологічних основ щодо розкриття та розслідування цієї категорії кримінальних правопорушень. Також правоохоронним органам необхідно налагодити концептуальну взаємодію з криптовалютними компаніями з метою блокування незаконної та протиправної діяльності у блокчейн платформах. Вирішення цієї проблеми має комплексний характер та вимагає розробки стратегії, направленої на запобігання використанню злочинцями нових сучасних фінансових механізмів.

Серед пріоритетних напрямків розвитку міжнародної кримінально-правової політики у сфері попередження використання криптовалют у злочинній діяльності виділяється: визначення моделі податкового адміністрування криптовалюти та правового статусу криптовалют; обов'язкове ліцензування діяльності у сфері обігу криптовалют (біржових сервісів, обмінних площадок, компаній, які випускають токени); встановлення міжнародних стандартів протидії легалізації злочинних доходів та фінансуванню тероризму. Також доцільно створити міжнародну базу даних про осіб, які займаються незаконним обігом та застосуванням цифрових фінансових активів в контексті технологій, що використовуються у протиправній діяльності. В нашій країні в умовах інституційного становлення новоствореного у 2021 році правоохоронного органу – Бюро економічної безпеки України [6], гостро стоїть питання утворення в його складі спеціального підрозділу, до компетенції якого слід віднести проведення розслідування протиправної діяльності з криптовалютами.

Використана література

1. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.

2. Гребенюк М.В., Черняк А.М. Проблеми протидії організованій злочинності у сфері цифрової економіки. *Підприємництво, господарство і прав*о. 2019. №3. С. 297-303.

3. Казначеєва Д.В., Дорош А.О. Кримінальні правопорушення у сфері обігу критовалюти. *Вісник кримінологічної асоціації У*країни. 2021. № 2 (25). С. 149-157.

4. Клименко О.А., Гуцалюк М.В. Кримінальний опортунізм кіберзлочинності як загроза національній безпеці України: наукові праці Національного авіаційного університету. *Повітряне і космічне право*. 2021. № 1(58). С. 177-184.

5. US DOJ To Bolster Newly Created “National Cryptocurrency Enforcement Unit” URL: https://cryptodaily.co.uk/2021/10/US-DOJ-To-Bolster-Newly-Created-National-Cryptocurrency-Enforcement-Unit

6. Про Бюро економічної безпеки України: Закон України від 28.01.21 р. № 1150. *Відомості Верховної Ради України.* 2021. № 23. Ст. 197. URL: https://zakon.rada.gov.ua/laws/ show/1150-20#Text

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~