УДК [351/75:324:342.9] (477)
DOI https://doi.org/10.24144/2307-3322.2025.92.4.41

ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ ПРИ РОЗКРИТТІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ЩО ВЧИНЯЮТЬСЯ У СФЕРІ ВІРТУАЛЬНИХ АКТИВІВ

Крижановський А.С.,
кандидат юридичних наук, доцент,
доцент кафедри міжнародного та кримінального права,
Національний університет «Львівська політехніка»
ORCID: 0000-0002-2432-5286

Крижановський А.С. Особливості проведення оперативно-розшукових заходів при розкритті кримінальних правопорушень, що вчиняються у сфері віртуальних активів.

У статті на підставі комплексного системного підходу розглянуто особливості проведення оперативно-розшукових заходів при розкритті кримінальних правопорушень, що вчиняються у сфері віртуальних активів. Актуальність теми дослідження обумовлена тим, що цифровізація економіки та, зокрема, фінансового сектора, обумовлює зміни в архітектурі фінансових потоків і механізмах регулювання. Розширення спектра фінансових інструментів, доступних завдяки новим технологіям, супроводжується оптимізацією витрат транзакцій, підвищенням ефективності ринкових процесів і виникненням принципово нових загроз, пов'язаних з потенційним зловживанням досягненнями технологічного прогресу в злочинних цілях. Об'єктом дослідження є суспільні відносини, що виникають у процесі вчинення кримінальних правопорушень у сфері віртуальних активів, а також діяльність, що здійснюється під час розкриття та розслідування таких правопорушень. Предметом дослідження виступають закономірності механізму кримінального правопорушення вчиненого щодо та з використанням віртуальних активів, і засновані на пізнанні даних закономірностей, особливості їх розкриття та розслідування. Зазначено, що середовище віртуальних активів має унікальний криміналістичний потенціал як джерело структурованих даних, що дозволяють змоделювати механізм злочинної діяльності. Це зумовлено її властивостями: децентралізацією, незмінністю транзакцій, прозорістю блокчейну та псевдо анонімністю учасників. Зазначені показники формують стійкі цифрові сліди, які за коректної інтерпретації стають основою встановлення причинно-наслідкових зв'язків, ідентифікації суб'єктів і доведення їх причетності до протиправних діянь. Цінність криміналістично значущої інформації у сфері віртуальних активів визначається її здатністю мінімізувати невизначеність у процесі розслідування, проте її ефективне використання потребує адаптації традиційних методів до специфіки технологій віртуальних активів. Актуальність, точність і повнота даних є ключовими критеріями, а їх аналіз має спиратися на принципи критичного мислення, міждисциплінарний підхід і інтеграцію сучасних інструментів.

Ключові слова: блокчейн, інформація, ідентифікації, інформаційні технології, трансакція, оперативно-розшукові заходи.

Kryzhanovskyi A.S. Features of conducting operational-investigative measures in the detection of criminal offenses committed in the field of virtual assets.

Based on a comprehensive systematic approach, the article examines the peculiarities of conducting operational-investigative measures in the detection of criminal offenses committed in the field of virtual assets. The relevance of the research topic is due to the fact that the digitalization of the economy and, in particular, the financial sector, causes changes in the architecture of financial flows and regulatory mechanisms. The expansion of the range of financial instruments available thanks to new technologies is accompanied by the optimization of transaction costs, increased efficiency of market processes, and the emergence of fundamentally new threats associated with the potential abuse of technological progress for criminal purposes. The object of the study is the social relations that arise in the process of committing

criminal offenses in the field of virtual assets, as well as the activities carried out during the detection and investigation of such offenses. The subject of the study is the patterns of the mechanism of criminal offenses committed against and using virtual assets, and is based on the knowledge of these patterns, the peculiarities of their detection and investigation. It is noted that the virtual asset environment has unique forensic potential as a source of structured data that allows the mechanism of criminal activity to be modeled. This is due to its properties: decentralization, immutability of transactions, transparency of the blockchain, and pseudo-anonymity of participants. These indicators form stable digital traces, which, when correctly interpreted, become the basis for establishing cause-and-effect relationships, identifying subjects, and proving their involvement in illegal activities. The value of criminally significant information in the field of virtual assets is determined by its ability to minimize uncertainty in the investigation process, but its effective use requires the adaptation of traditional methods to the specifics of virtual asset technologies. The relevance, accuracy, and completeness of data are key criteria, and their analysis must be based on the principles of critical thinking, an interdisciplinary approach, and the integration of modern tools.

Key words: blockchain, information, identification, information technology, transaction, operational-investigative measures.

Постановка проблеми. Сучасний етап трансформації політичної, економічної та соціальної сфер характеризується тенденцією зростання злочинності у сфері інформаційних технологій, що становить серйозний виклик для правоохоронних органів. Кримінальні правопорушення з віртуальними активами демонструють неспроможність традиційних методів боротьби перед загрозою, яка динамічно розвивається. Виникає необхідність у розробці і впровадженні нових алгоритмів, що регламентують діяльність підрозділів, уповноважених здійснювати оперативно-розшукову діяльність. Удосконалення потребує нормативно-правовий інструментарій оперативно-розшукової діяльності та тактичні і стратегічні методи протидії злочинності.

Мета дослідження визначити особливості проведення оперативно-розшукових заходів при розкритті кримінальних правопорушень, що вчиняються у сфері віртуальних активів.

Стан опрацювання проблематики. Окремі питання розкриття кримінальних правопорушень у сфері віртуальних активів розглядали: Р.О. Баранов; Б.Г. Безгинський; Л.В. Герасименко; М.В. Гуцалюк; С.В. Демедюк; Т.Л. Дмитренко; Т.Є. Зелькіна; Л.В. Кальченко, Н.А. Лугіна; Є.В. Панченко; О.О. Саєнко; Б.Б. Теплицький; К.П. Шевчишена та інші вчені. Економічна інтеграція України до Європейського Союзу вимагає адаптації законодавства, що відповідно потребує проведення міждисциплінарних науково-правових досліджень, у тому числі щодо оперативно-розшукової діяльності з розкриття та розслідування кримінальних правопорушень у сфері віртуальних активів.

Виклад основного матеріалу. Прийняття у першому читанні проєкту закону «Про внесення змін до Податкового кодексу України та деяких інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні» сприяє легалізації віртуальних активів [1]. Поява нових засобів комунікації та технологій обумовлює необхідність розробки нових чи вдосконалення існуючих оперативно-розшукових заходів. Цифрова реальність визначила нові тенденції у розвитку криміналістичної науки з урахуванням потреби виявляти закономірності між слідами і злочинною подією, що сталася у нематеріальній складно структурованій системі блокчейну.

Традиційне трактування об'єктів оперативно-розшукової діяльності, що включає осіб, предмети, події і відомості, демонструє обмежену застосовність у контексті кримінальних правопорушень у сфері віртуальних активів. Висока технологічність актуалізує потребу у розробці інноваційних методів виявлення і всебічного вивчення нових об'єктів, в умовах дефіциту вихідної інформації.

В.В. Саєнко зазначає, що поза увагою науковців залишаються питання: сутності злочинної діяльності пов'язаної з використанням віртуальних активів; поняття віртуальних активів як складової криміналістичної характеристики окремих кримінальних правопорушень; обставин, що підлягають встановленню під час розслідування кримінальних правопорушень, пов'язаних з використанням віртуальних активів [2, с. 290].

Вивчення типових методів вчинення кримінальних правопорушень у сфері віртуальних активів, дозволило виділити дві принципово різні категорії протиправних діянь: дії спрямовані на віртуальні активи як безпосередній предмет зазіхання, та дії, у яких віртуальні активи застосовуються як інструмент реалізації протиправних цілей.

К.О. Юсупова, В.В. Юсупов, Р.П. Марчук зазначають, що у розслідуванні злочинів, пов'язаних з використанням віртуальних активів, типовими оперативно-розшуковими діями є огляд, обшук, допит, залучення експерта [3, с. 326]. На початковому етапі розкриття та розслідування ключову роль відіграє первинна перевірка і оцінка інформації, що надійшла про дії, які мають кримінальний характер. За правопорушеннями першої категорії підставою проведення перевірочних заходів є заяви від фізичних і юридичних осіб, щодо яких було реалізовано протиправну схему. Після отримання заяви про кримінальне правопорушення, де завдано значної матеріальної шкоди, проводиться опитування особи, яка постраждала від протиправного діяння.

Під час перевірки шахрайських схем у ході опитування встановлюються обставини знайомства з передбачуваним зловмисником, наприклад, через соціальні мережі, месенджери чи інвестиційні онлайн-платформи. Виявляється характер і змістом повідомлень, що передували здійсненню транзакцій. Уточняються технічні деталі здійснення транзакцій, включаючи тип валютних ринків, що використовуються, види віртуальних активів, обсяги транзакцій, адреси гаманців відправника і одержувача. У опитуваного запитується документальне підтвердження факту здійснення транзакцій, скріншоти транзакцій, дані оплачених ордерів на біржах (ринках) віртуальних активів [4].

Типовим є випадок, коли потерпілий, введений в оману обіцянками швидкого збагачення, переводить віртуальні активи на гаманець віртуальних активів (далі – гаманець), контрольований зловмисниками. Потерпілий, довіряючи отриманій інформації, переказав активи на вказаний гаманець, після чого зв'язок із шахраями перервався, а активи було втрачено.

При опитуванні постраждалих від випадків маніпулювання ринком віртуальних активів у протоколі фіксується, за допомогою яких ресурсів особа отримала інформацію про конкретний віртуальний актив, ICO-проект або осіб, підозрюваних у маніпулюванні ринком. Джерела інформації можуть включати рекламні кампанії у соціальних мережах, рекомендації та просування від впливових осіб, блогерів і аналітиків. Інформація поширюється у закритих групах або каналах у месенджерах, де надаються інсайдерські відомості чи торгові рекомендації.

На думку А.В. Ковальського, одним із основних завдань оперативно-розшукової діяльності є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп, відповідальність за які передбачена Кримінальним кодексом України, яке виконується із застосуванням оперативних та оперативно-технічних засобів [5, с. 448].

Доцільно долучати до опитування скріншоти: листування з передбачуваними зловмисниками; рекламних оголошень, обіцянок, торгових сигналів і інших матеріалів; розвантаження даних ордерів на віртуальних ринках; скріншоти графіків зміни цін; виписки з гаманців; документи, що засвідчують особу і інші дані, надані організаторам ICO або учасникам маніпулятивних схем.

За кримінальними правопорушеннями другої категорії, які характеризуються високою волатильністю цін (показник, який характеризує тенденції зміни ринкових цін і доходів упродовж певного часу); можливість шахрайства; відсутність гарантій повернення реальних коштів, вкладених у криптовалюти; неповнота або недостовірність інформації, де віртуальні активи є засобом здійснення злочинної діяльності та де джерелом оперативної інформації є дані про транзакції та підозрілу активність, пов'язану з гаманцями віртуальних активів, доцільно організувати опитування робітника фінансової організації для встановлення обставин, що сприяють розкриттю кримінального правопорушення [6, с. 246].

При виявленні транзакції, яка відповідає певним критеріям підозрілості, відмічається моніторингом і спрямовується на подальше розслідування. У ході розслідування аналізується додаткова інформація про транзакцію, контрагентів і клієнта. Під час опитування уповноважений співробітник може дати пояснення щодо цих обставин. Після отримання інформації про подію в ході перевірки діянь першої та другої категорії доцільно організувати оперативно-розшукові заходи [7].

Аналіз отриманих даних у результаті такої діяльності дозволяє виявляти потенційні загрози та нові тенденції у злочинній діяльності, планувати оперативні заходи. У ході наведення довідок на адресу ринків віртуальних активів і обмінників можуть бути надіслані запити для встановлення особи власників гаманців, які беруть участь у злочинних транзакціях.

Оперативним співробітником при наведенні довідок може бути направлений запит: Інтернет-провайдерам, іншим організаціям для встановлення IP-адреса і інших технічних даних, пов'язаних з використанням сервісів віртуальних активів; реєстраторам доменних імен і хостинг-провайдерам для встановлення власників веб-сайтів і доменів, які використовуються в злочинних

цілях; у банківські організації для отримання інформації про транзакції, пов'язані з виведенням віртуальних активів у фіатні гроші.

Оперативно значущі відомості при виявленні злочинної діяльності можна отримати з самої інфраструктури віртуальних активів. Транзакції з токенами і більшістю інших віртуальних активів засновані на існуванні публічного реєстру – блокчейну, в якому вони підтверджуються та записуються в хронологічному порядку для забезпечення цілісності системи. Блокчейн фіксує всі транзакції, проведені власником певного гаманця, у хронологічному порядку [8, с. 118].

При наведенні довідок оперативний співробітник може отримати історію транзакцій віртуального активу, включаючи адреси всіх користувачів, з якими він здійснював транзакції, дату, час і точну суму переказу. Це є корисним критерієм за одночасного аналізу великої кількості транзакцій. Комплексний аналіз отриманого масиву даних і його зіставлення з відомостями з інших джерел має значення для виявлення ознак злочинної діяльності, ідентифікації причетних осіб і встановлення їх ролі у вчиненні правопорушення.

За кримінальними правопорушеннями другої категорії при наведенні довідок корисно ввести наявні дані про фігуранта в пошукові браузери Інтернету, оскільки особи, які беруть участь у незаконній торгівлі, публікують свою адресу, пов'язуючи її з обліковим записом і псевдонімом. На форумах або розділах коментарів спеціалізованих сайтів можуть бути встановлені додаткові відомості.

Аналогічний метод використовується для отримання інформації в мережі *DarkNet*, де існує ряд форумів, на яких встановлюються відомості про приховані сервіси, їх адреси, коментарі щодо якості обслуговування, псевдоніми успішних продавців. За допомогою моніторингу форумів і соціальних мереж, де обговорюються питання інвестицій у віртуальних активах, є можливість встановити нелегальні платформи, які пропонують послуги обміну чи інвестування, але не зареєстровані в установленому порядку [9, с. 354]. Вивчення діяльності криптоміксерів, що використовуються для приховання походження та руху активів, здатне бути ефективним із застосуванням зазначеного методу.

Аналіз трафіку, метаданих транзакцій і інформації про сервери, що надають послуги мікшування, дозволяє ідентифікувати пов'язані з ними адреси і оцінювати обсяги транзакцій, що обробляються. Наприклад, виявлення згадок про конкретного криптоміксера у зв'язку з відмиванням коштів, отриманих в результаті кібер здирства, може стати початковою ланкою в ланцюзі транзакцій, які здійснювалися причетними особами. Це зумовлено тим, що операційна діяльність зазначених структур заснована на системі репутаційного контролю, що й у нелегітимних онлайн-маркетплейсів, рентабельність яких залежить від зворотного зв'язку учасників ринку на профільних форумах.

Незважаючи на поширення інструментів анонімності і дистанційний характер взаємодії у кіберпросторі, зберігається можливість встановлення стійких зв'язків між учасниками незаконної діяльності. Це обумовлено необхідністю формування довірчих відносин, оскільки особа, яка здійснює легалізацію доходів, отриманих злочинним шляхом, з високою ймовірністю буде прагнути встановлення контролю над фінансовими потоками і не зможе делегувати подібні функції особі, яка не викликає довіри.

Необхідно враховувати, що аналіз інформації, доступної з відкритих джерел, включаючи дані про спосіб життя, активи, місця проживання, комерційну чи соціальну активність осіб, яких підозрюють, дозволяє отримати цінні відомості. Ненавмисна публікація інформації в соціальних мережах, що розкриває обставини життя і діяльності, зв'язки осіб, причетних до кримінального правопорушення, може надати істотну допомогу у розслідуванні злочинів, пов'язаних із використанням віртуальних активів.

При вивченні соціальних мереж слід звертати увагу на те, що в кожному Інтернет-ресурсі іманентно присутні як мінімум два рівні даних, які можуть бути використані при проведенні оперативно-розшукових заходів. Це рівень контенту, що включає інформацію, опубліковану користувачем. Розміщені візуальні матеріали здатні надати значний обсяг відомостей про суб'єкта, включаючи фізіологічні дані, інформацію про соціокультурне оточення, географічне розташування, соціальний статус, ідеологічні переконання, методологію інформаційної безпеки [10, с. 53].

Під першим рівнем знаходиться другий рівень, представлений метаданими, які можуть повідомляти інформацію про комп'ютерний пристрій, за допомогою якого було опубліковано контент, користувача або описові дані файлів. Характерним прикладом таких метаданих є EXIF-дані

(формат файлів зображень з можливістю обміну), які спочатку містяться у відео або фотоматеріалах і описують обладнання та параметри, використані при створенні відео або фотозображення. Дана інформація дозволяє встановити емпіричні факти або сформувати аналітичні висновки про суб'єктів чи організації, пов'язані з цими файлами або акаунтами в соціальних мережах, де вони були розміщені.

Поряд із загальнодоступними пошуковими системами для виявлення специфічних типів даних застосовуються спеціалізовані інструменти. Програма Shodan орієнтована на пошук пристроїв, підключених до Інтернету, таких як веб-камери, принтери, VoIP-пристрої та маршрутизатори. Даний ресурс дозволяє ідентифікувати потенційно скомпрометовані пристрої, що використовуються для проведення транзакцій або зберігання криптографічних ключів, та сприяти розслідуванню кримінальних правопорушень у сфері віртуальних активів.

Іншим прикладом є програма NameCHK, що надає можливість перевірки доступності імені користувача у різних онлайн-сервісах. Функціонал програми дозволяє виявляти зв'язок між псевдонімами, використовуваними зловмисниками у різних контекстах. Слід згадати про програму Pipl, яка представляє аналітичний інструмент. Він дозволяє шукати збіги в мережі Інтернет за різними критеріями, включаючи імена, адреси електронної пошти або номери телефонів, що надає можливість агрегувати велику інформацію про фігурантів з різноманітних відкритих джерел.

Платформи, такі як GitHub, можуть застосовуватися для пошуку і аналізу програмного коду, що стосується розробки і експлуатації шахрайських проектів або шкідливого програмного забезпечення, призначеного для розкрадання віртуальних активів.

У тактичному плані дані інструменти OSINT дозволяють оперативним співробітникам формувати цілісне уявлення про діяльність зловмисників, пов'язаних із віртуальними активами, відстежувати рух коштів, ідентифікувати пов'язаних осіб і виявляти вразливість у системах безпеки. Використання описаних технологій разом із класичними методами розслідування підвищує ефективність боротьби зі правопорушеннями у сфері віртуальних активів.

Оперативно-розшуковий захід дослідження предметів і документів розглядається як елемент оперативно-розшукової діяльності, набуває особливої актуальності при документуванні діяльності організованих злочинних спільнот. Сутність заходу полягає у візуальному вивченні, аналізі і дослідженні властивостей предметів і документів з метою вилучення значущих відомостей, встановлення їх справжності, виявлення ознак фальсифікації, визначення зв'язку з кримінальним правопорушенням, що розслідується [11, с. 5].

Практична реалізація цього оперативно-розшуковий захід потребує врахування специфіки кримінальних правопорушень у сфері віртуальних активів, які характеризуються високим ступенем цифровізації та використанням сучасних інформаційних технологій. Коло предметів і документів, що підлягають дослідженню, включає традиційні матеріальні об'єкти і електронні носії інформації. При розкритті кримінальних правопорушень у сфері віртуальних активів дослідження предметів і документів спрямоване на встановлення факту розкрадання, шахрайства чи вимагання, виявлення обставин, які сприяли вчиненню правопорушення.

При розкритті правопорушень, вчинених з використанням віртуальних активів, дослідження предметів і документів орієнтоване на встановлення зв'язку між транзакціями і злочинною діяльністю, виявлення осіб, причетних до вчинення правопорушення. Особливого значення набуває вивчення електронних пристроїв, що використовуються для здійснення транзакцій, на яких можуть міститися відомості про гаманці, транзакції, IP-адреси і інші дані, що дозволяють встановити особи злочинців та їх спільників.

У процесі дослідження предметів і документів необхідно враховувати можливість використання фігурантами різних методів приховування інформації, таких як шифрування даних, використання стенографії, видалення файлів. Для проведення всебічного дослідження необхідно залучати кваліфікованих фахівців у галузі інформаційних технологій, які мають необхідні знання та навички.

Для виявлення злочинної діяльності, пов'язаної з віртуальними активами, може проводитися комплекс негласних оперативно-розшукових і оперативно-технічних заходів. Ключовою умовою є реконструкція цифрового майданчика, у якому функціонують фігуранти, з точним відтворенням технічних параметрів, соціокультурних норм, притаманних таким торговим площадкам. Технологічна достовірність досягається через комбінацію блокчейн-аналітики, моніторингу *DarkNet*, впровадження у закриті форуми, що дозволяє виявити актуальні тренди.

Організовані злочинні спільноти використовують багаторівневу систему верифікації нових учасників кримінального ринку, що включає перевірку історії гаманців на зв'язок із сумнівними адресами, пошук згадок платформи в закритих джерелах, тестування на стійкість до DDoS-атак і спроб злому. Технологічна достовірність стає не самоціллю, а інструментом формування кримінального середовища, де кожна дія суб'єкта може бути використана для нейтралізації.

Ключовим елементом успішного впровадження є демонстрація агентом професійної компетентності і операційної надійності, що необхідно для формування у цільових суб'єктів сприйняття потенційної вигоди та мінімізації ризиків при взаємодії. Цей підхід ґрунтується на принципах соціальної довіри, характерної для закритих кримінальних спільнот, де встановлення ділових відносин потребує підтвердження репутації і відповідності неформальним нормам. Проте оперативна діяльність у таких умовах пов'язана з високим ступенем невизначеності, зумовленої динамікою нелегальних ринків, включаючи мінливість методів комунікації, ескалацію підозрілості серед учасників і використання кримінальними групами контррозвідувальних механізмів. Ефективність подібних операцій безпосередньо залежить від психологічної підготовки оперативних співробітників, їх вміння балансувати між необхідністю збирання доказів і уникнення провокаційних дій. Це наголошує на етико-правовій складності застосування подібних методів у межах чинного законодавства.

Перспективним напрямом отримання оперативно значущої інформації у правоохоронних органах Європейського Союзу є використання методу «контроль на старті», що дозволяє виявляти транзакції у тимчасових сховищах, що дає змогу відстежувати потенційно незаконні операції ще до включення до блокчейну. Застосування даного методу вимагає спеціалізованого програмного забезпечення і доступу до вузлів мережі блокчейн, сприяє підвищення ефективності діяльності запобігання та розкриття кримінальних правопорушень, пов'язаних з використанням віртуальних активів.

Висновки. Сучасний етап розвитку злочинності, пов'язаної з віртуальними активами, характеризується трансформацією оперативно-розшукової діяльності, обумовленої технологічними викликами та необхідністю адаптації традиційних методів до цифрової реальності. Аналіз представленого матеріалу дозволяє констатувати, що кримінальні правопорушення, спрямовані на віртуальні активи як об'єкт зазіхання або використовують їх як інструмент, формують потребу у вирішенні нових завдань до збирання, дослідження і верифікації даних.

Анонімність транзакцій і децентралізований характер блокчейну суттєво ускладнюють ідентифікацію суб'єктів злочинної діяльності, що актуалізує необхідність розробки спеціалізованих алгоритмів, які інтегрують методи блокчейн-аналітики. Використання платформ для візуалізації зв'язків між гаманцями та цифровими ідентифікаторами демонструє ефективність міждисциплінарного підходу, що поєднує криміналістичні методики з технологіями великих даних.

Класифікація кримінальних правопорушень у сфері віртуальних активів на дві категорії – зазіхання на цифрові активи і їх використання з протиправною метою визначає диференціацію тактичних прийомів. У першому випадку пріоритет надається ретроспективному аналізу транзакцій через публічні реєстри блокчейна із встановленням ланцюжків переміщення активів, тоді як у другому центр зміщується на виявлення інфраструктурних елементів, що потребує застосування превентивних оперативних моделей.

Часткове зняття анонімності транзакцій через аналіз соціальних медіа та метаданих здатне стати ключовою ланкою у встановленні причетних осіб. Це потребує розвитку міжвідомчих баз даних і алгоритмів машинного навчання для обробки масивів неструктурованої інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Проєкт закону «Про внесення змін до Податкового кодексу України та деяких інших законодавчих актів України щодо врегулювання обороту віртуальних активів в Україні» (10225-д). Верховна Рада України. URL: blob:https://itd.rada.gov.ua/d050bbf7-6a40-4750-95ef-edbfd9db0ba6.
2. Саєнко В.В. Аналіз стану наукового дослідження проблем розслідування кримінальних правопорушень, пов'язаних з використанням віртуальних активів. *Аналітично-порівняльне правознавство*. 2025. № 4. С. 280-294. DOI https://doi.org/10.24144/2788-6018.2025.04.3.41.
3. Юсупова К.О., Юсупов В.В., Марчук Р.П. Особливості проведення окремих слідчих (розшукових) дій під час розслідування кримінальних правопорушень, пов'язаних з викорис-

танням криптовалюти. *Аналітично-порівняльне правознавство*. 2025. № 5. С. 322-327. DOI https://doi.org/10.24144/2788-6018.2025.05.3.47.
4. Про віртуальні активи: Закон України від 17.02.2022 р. № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20/conv#n6.
5. Ковальський А.В. Проблемні аспекти негласних заходів оперативних підрозділів під час виявлення та розшуку віртуальних активів, пов'язаних із кримінальними правопорушеннями. *Юридичний науковий електронний журнал*. 2024. № 10. С. 447-450. DOI https://doi.org/10.32782/2524-0374/2024-10/103.
6. Ковалів М.В., Єсімов С.С., Ярема О.Г. Інформаційне право України: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2022. 416 с. URL: http://dspace.lvduvs.edu.ua/handle/1234567890/4844.
7. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № 2135-XII. URL: https://zakon.rada.gov.ua/laws/card/2135-12.
8. Терлюк О.І. Правове регулювання блокчейн-технології у публічному управлінні: аспекти міжнародного та українського досвіду використання. Монографія. Львів: Растр-7, 2024. 260 с. URL: https://shron1.chtyvo.org.ua/Terliuk_Oleksii/Pravove_rehuliuvannia_blokcheintekhnolohii_u_publichnomu_upravlinni_aspekty_mizhnarodnoho_ta_ukrain.pdf?PHPSESSID=iqn1qivnmj1lvo5ebsohn2p7j1.
9. Єсімов С.С. Цифрові платформи у контексті надання публічних послуг. *Аналітично-порівняльне правознавство*. 2024. № 4. С. 352-357. DOI https://doi.org/10.24144/2788-6018.2024.04.56.
10. Yesimov S., Borovikova V. Methodological foundations of information security research. *Social & Legal Studios*. 2023. Vol. 6, № 1. P. 49-55. DOI: 10.32518/sals1.2023.49.
11. Худик А.М. Правове регулювання обігу віртуальних активів та їх використання в кримінальному праві і процесі. *Академічні візії.* 2025. Випуск 42. С. 1-7. URL: https://orcid.org/0000-0003-3174-8428.