Криміналістична характеристика кримінальних правопорушень, пов'язаних з незаконним обігом віртуальних активів

Дмитро Нестеров *

* Спеціаліст-консультант у сфері криптоаналітики (NDA), м. Харків, Україна,
ORCID: https://orcid.org/0009-0008-3252-4649, e-mail: nesterov.dmitriy85@ukr.net

DOI: 10.32353/khrife.2.2026.12 УДК 343.985(477)
Надійшло 14.05.2026 / Рецензовано 26.05.2026 / Прийнято до друку 24.06.2026 /
Доступно онлайн 30.06.2026

Мета статті — розкрити особливості криміналістичної характеристики злочинів, пов'язаних з незаконним обігом віртуальних активів, а також визначити основні елементи механізму їх скоєння. Для досягнення поставленої мети застосовано комплекс загальнонаукових і спеціально-юридичних методів пізнання, зокрема діалектичний, системно-структурний, формально-юридичний, порівняльно-правовий, логіко-семантичний, аналізу й синтезу, моделювання й узагальнення. Статтю присвячено дослідженню криміналістичної характеристики кримінальних правопорушень, пов'язаних з незаконним обігом віртуальних активів, що в умовах глобальної цифровізації та стрімкого розвитку інформаційних технологій набувають дедалі більшої суспільної небезпеки. Актуальність теми обумовлена активним використанням криптовалют, децентралізованих фінансових сервісів, анонімних платіжних інструментів і технологій штучного інтелекту в механізмах учинення шахрайств, кіберзлочинів і легалізації доходів, одержаних злочинним шляхом. Зростання рівня транснаціональної кіберзлочинності, поширення фішингових схем, користування міксерами, тумблерами, офшорними юрисдикціями та платформами із наскрізним шифруванням створюють істотні труднощі для правоохоронних органів під час виявлення, документування й розслідування таких правопорушень. Особливу увагу приді-

лено проблемам формування доказової бази, пов'язаним з віртуальною природою цифрових слідів і складністю ідентифікації осіб, причетних до незаконних операцій з віртуальними активами. У результаті проведеного дослідження визначено, що віртуальні активи як предмет злочинного посягання формують специфічний механізм злочинної діяльності, для якого характерними є високий рівень латентності, транскордонність, застосування сучасних інформаційних технологій і складність локалізації місця вчинення кримінального правопорушення. Обґрунтовано, що вирішальне значення для розслідування мають цифрові сліди, що їх містять блокчейн, електронні гаманці, акаунти користувачів, пам'ять комп'ютерної техніки, месенджери, соціальні мережі, бази даних операторів зв'язку й інтернет-провайдерів. Проаналізовано найбільш поширені способи скоєння злочинів, пов'язаних з незаконним обігом віртуальних активів, поміж яких фішингові атаки, злам криптовалютних бірж і електронних гаманців, користування фейковими платформами, маніпуляції з токенами, шахрайські інвестиційні проєкти, DeFi-експлойти, NFT-шахрайство й легалізація доходів за допомогою криптовалютних сервісів і онлайн-казино. Доведено, що значну частину таких правопорушень здійснюють транснаціональні організовані злочинні угруповання із чітким розподілом ролей між учасниками. Аргументовано, що особа правопорушника в цій категорії злочинів характеризується високим рівнем цифрової компетентності, спеціальними знаннями у сфері інформаційних технологій, програмування або фінансів і орієнтуванням на отримання матеріальної вигоди. Запропоновано класифікувати суб'єктів таких кримінальних правопорушень як технічно підготовлених спеціалістів, професійних кіберзлочинців і осіб з легальним професійним статусом, які застосовують свої знання для реалізації злочинних схем. Зроблено висновок, що кримінальні правопорушення, пов'язані з незаконним обігом віртуальних активів, є складним багаторівневим явищем, яке поєднує ознаки кіберзлочинності, економічної злочинності та транснаціональної організованої діяльності. Наголошено на необхідності подальшого розвитку криміналістичних методик розслідування, удосконалення законодавчого регулювання обігу віртуальних активів і підвищення рівня технічної підготовки правоохоронних органів у сфері роботи із цифровими доказами й технологіями блокчейну.

Ключові слова: *віртуальний актив; блокчейн; транскордонні злочини; легалізація (відмивання) грошей, здобутих злочинним шляхом; шахрайство; крадіжка; криміналістична характеристика; незаконний обіг.*

Постановка наукової проблеми

Технологічні інновації стали рушієм економічного й соціального прогресу, але ті самі інновації вивели на ринок чинники, що сприяють кібершахрайству, знижують бар'єри, розширюють охоплення та дають змогу шахраям масштабувати операції. Багато фінансових і нефінансових послуг швидко поширилися в онлайн-середовищі під час пандемії *COVID-19*. Як підкреслено у спільній публікації *FATF* (Міжнародна група з протидії відмиванню «брудних» грошей, англ. *Financial Action Task Force*), Егмонтської групи підрозділів фінансової розвідки й Інтерполу щодо незаконних фінансових потоків від кібершахрайства, кібершахрайство та подібні злочини переживають вибухове зростання, спричинене новітніми технологіями — штучним інтелектом (далі — *ШІ*) і діпфейками на його основі [1].

Держфінмоніторинг також наголошує, що розвиток фінансової інфраструктури підвищує труднощі в боротьбі з шахрайством. Зростаюче застосування віртуальних активів (далі — *ВА*), а також каналів миттєвих і транскордонних платежів з недостатніми цілеспрямованими заходами пом'якшення наслідків дають змогу переказувати доходи до їх виявлення або втручання. Часто масштабні схеми кібершахрайства здійснюють або полегшують транснаціональні організовані злочинні угруповання: такими схемами управляють за допомогою спеціалізованих шахрайських центрів [2]. Аналогічна ситуація із маскуванням незаконних операцій через їх проведення за допомогою ВА склалася на більшості чорних ринків (продаж зброї, наркотиків, надання незаконних послуг тощо) і у сфері легалізації (відмивання) злочинних доходів.

Держфінмоніторинг фіксує такі випадки відмивання доходів, отриманих від шахрайських дій і кіберзлочинів: застосування технологій ШІ з метою незаконного проходження дистанційної ідентифікації та отримання доступу до рахунку клієнта; умисна підробка документів з унесення коштів на депозит для шахрайського заволодіння грошовими коштами банківської установи; шахрайський продаж фізичною особою об'єктів комерційної нерухомості, до будівництва яких вона не мала законного відношення, за готівкові кошти; шахрайське заволодіння готівковими й безготівковими коштами громадян під виглядом збору коштів на потреби Збройних сил України; заволодіння коштами фізичних осіб шляхом обману або зловживання довірою (продаж відсутніх товарів через соціальних мереж) з подальшим виведенням коштів на криптовалютну біржу; користування підробленим вебсайтом державного органа для доступу до особистих даних і банківських рахунків з метою незаконного списання коштів; застосування фішингових листів для отримання доступу до банківського рахунку жертви та здійснення незаконних переказів [3].

1 Cyber-Enabled Fraud. Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks. February 2026 / FATF : web. 9 p. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Cyber-Enabled-Fraud%E2%80%93Digitalisation-and-ML-TF-PF-Risks.pdf.coredownload.inline.pdf (дата звернення: 11.04.2026).

2 Типологічне дослідження на тему: «Ризики та загрози легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму в умовах військової агресії російської федерації — 2025» : затв. наказ. Держфінмоніторингу України від 22.12.2025 р. № 116. URL: https://surl.li/spkkxl (дата звернення: 11.04.2026).

3 Там само.

Непоодинокі також випадки відмивання злочинних доходів із застосуванням ВА: проведення операцій з криптоактивами; користування стороннім сервісом обміну за допомогою звичайних поточних рахунків, не призначених для такої діяльності, із залученням неповнолітніх осіб та іноземних громадян; застосування ВА як викупу за розблокування роботи компаній-нерезидентів, які постраждали внаслідок кібератак; використання фейкових проєктів з криптотрейдингу, що фактично є елементом фінансової піраміди, з метою шахрайського заволодіння коштами громадян України й іноземців [4].

Інтерпол також фіксує подібні тенденції у своїх юрисдикціях. За даними Інтерполу, широке користування платформами з наскрізним шифруванням (*E2EE*) у поєднанні зі складними юрисдикційними й технічними бар'єрами залишає слідчі «сліпі плями». Окрім того, роботі часто заважає обмежувальна або неадекватна політика зберігання даних (наприклад, на криптобіржах). На той час, коли слідчі запитують доступ до релевантних даних, вони часто вже недоступні.

Кіберзлочинності сприяє стійкість маркетплейсів і форумів даркнету. Ці платформи дедалі більше переплітаються з *E2EE* платформами в гібридну екосистему анонімності. Криптовалюти залишаються улюбленим методом оплати для кіберзлочинців, особливо під час атак програм-вимагачів.

Онлайн-шахрайство злочинних угруповань націлено як на окремих осіб, так і на організації — для отримання прибутків від таких схем, як інвестиційне шахрайство, компрометація електронної пошти (англ. *Business Email Compromise, BEC*) і шахрайство з онлайн-платіжними системами. Із упровадженням генеративного ШІ шахраї можуть персоналізувати методи соціальної інженерії та зробити їх більш переконливими.

Основною загрозою в ЄС залишаються програми-вимагачі: понад 120 активних брендів (за даними Європолу 2025 року). Модель вимагання продовжує зміщуватися від шифрування даних до тиску на жертв з метою оплати за нерозголошення їхніх даних.

Нові технології та монетизація. Злочинці швидко адаптуються до нових технологій, ускладнюючи роботу правоохоронних органів. Торгівля матеріалами сексуального насильства над дітьми заради фінансової вигоди зростає, як і багаторівневі моделі вимагання. Зростання кількості *CSAM* (англ. *Child Sexual Abuse Material* — матеріали, пов'язані із сексуальним насильством над дітьми) таких матеріалів, згенерованих ШІ, створює додаткові проблеми.

Використання криптовалют у кіберзлочинності швидко розвивається. Злочинці часто віддають перевагу користуванню послугами обміну, розташованими в юрисдикціях зі слабкими протоколами протидії відмиванню грошей (англ. *Anti-Money Laundering, AML*) або в офшорних фінансових центрах [5].

В умовах сьогодення особливої гостроти набуває питання нейтралізації правопорушень, пов'язаних з незаконним обігом ВА, які сьогодні є найбільш прогресивним і архітектурно складним пластом кіберзлочинності. Еволюція цього напряму нелегальної діяльності відбувається синхронно з розширенням масштабів цифрової економіки й упровадженням новітніх блокчейн-рішень.

4 Типологічне дослідження … . URL: https://surl.li/spkkxl (дата звернення: 11.04.2026).

5 IOCTA 2026 – The evolving threat landscape: how encryption, proxies and AI are expanding cybercrime. Internet Organised Crime Threat Assessment (IOCTA) 2026 / EUROPOL : web. 28 Apr 2026. DOI: 10.2813/5737847 (дата звернення: 11.04.2026).

Такі інструменти, як біткоїн, ефіріум, стейблкоїн, а також *DeFi*-сервіси і NFT (невзаємозамінний токен, англ. *Non-fungible Token*), дедалі частіше стають не лише об'єктами інвестування, а й основними елементами у схемах із легалізації тіньових капіталів, обходу механізмів фінансового моніторингу й матеріального забезпечення криміналітету [6] (зокрема, від міжнародних санкцій [7]).

Мета статті

Розкрити особливості криміналістичної характеристики злочинів, пов'язаних з незаконним обігом ВА, а також визначити основні елементи механізму їх скоєння.

Методи дослідження

Досягнення мети статті забезпечено комплексним застосуванням загальнонаукових і спеціально-юридичних методів пізнання. Діалектичний метод став у пригоді для з'ясування закономірностей, що їх виявляють в елементах криміналістичної характеристики злочинів, пов'язаних з незаконним обігом ВА.

Метод аналізу й синтезу допоміг в опрацюванні наукових джерел і практико-орієнтованих підходів щодо міжнародного й національного досвіду в розслідуванні транснаціональних економічних і кіберзлочинів, зокрема, пов'язаних з незаконним обігом ВА, а також під час виокремлення основних елементів криміналістичної характеристики злочинів, пов'язаних з незаконним обігом віртуальних активів (предмета злочину, обстановки, часу, місця, способів підготовки, скоєння та приховування злочинів, особи злочинця тощо).

Системно-структурний метод дав змогу сформувати цілісні елементи криміналістичної характеристики злочинів, пов'язаних з незаконним обігом ВА з транснаціональних економічних злочинів, кіберзлочинів і легалізації (відмивання) доходів, отриманих злочинним шляхом, з використанням віртуальних валют.

Формально-юридичний метод сприяв аналізу національних і міжнародних нормативних актів щодо обігу ВА, легалізації (відмивання) доходів, отриманих злочинним шляхом, і боротьби з кіберзлочинністю.

Логіко-догматичний (логіко-семантичний) метод застосовано для уточнення змісту категорій «спосіб готування до злочину», «спосіб учинення злочину», «спосіб приховування злочину», «сліди злочину» в контексті криміналістичної характеристики злочинів, пов'язаних з незаконним обігом ВА, а також для формулювання висновків.

Порівняльно-правовий метод став у пригоді для зіставлення наукових підходів до тактичного забезпечення взаємодії з потерпілими у провадженнях щодо тяжких і міжнародних злочинів, а також для врахування міжнародних стандартів у сфері поводження з потерпілими й захисту їхніх прав у контексті потенційних механізмів міжнародного кримінального правосуддя.

Метод моделювання допоміг окреслити типові способи готування, скоєння та приховування злочинів, пов'язаних з незаконним обігом ВА.

6 Щорічний звіт Департаменту кіберполіції Національної поліції України за 2025 рік / Кіберполіція України : офіц. вебсайт. 16.02.2026. URL: https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/ (дата звернення: 11.04.2026).

7 Crypto Crime in 2025 Was Primarily Driven by 694% Surge in State-Driven Sanctions Evasion Volume / Chainalysis : web. March 5, 2026. URL: https://live-chainalysis.pantheonsite.io/blog/crypto-sanctions-2026/ (дата звернення: 11.04.2026).

Метод узагальнення сприяв систематизації результатів опрацювання доктринальних джерел і практичних даних та формулюванню авторських висновків щодо елементів криміналістичної характеристики злочинів, пов'язаних з незаконним обігом ВА.

Аналіз основних досліджень і публікацій

Дослідження теоретичних аспектів скоєння злочинів, пов'язаних з незаконним обігом ВА, останнім часом дедалі частіше цікавлять учених, оскільки їх кількість невпинно зростає, як і кількість осіб, у чиє життя увійшли цифрові активи.

Елементи криміналістичної характеристики злочинів, пов'язаних з незаконних обігом ВА, фрагментарно розкрито у працях В. Божика [8], А. Долгова [9], Б. Деревянка [10], І. Завидняк [11], М. Карчевського зі співавторами [12], Е. Малютіна [13], Я. Неділька [14], О. Кремінського [15], А. Мовчана й В. Козія [16],

8 Божик В. І. Криміналістична характеристика легалізації майна, одержаного внаслідок ухилення від сплати податків: елементи та механізм злочинної діяльності. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2026. Вип. 93. Ч. 5. С. 28—34. DOI: 10.24144/2307-3322.2026.93.5.3 (дата звернення: 08.04.2026).

9 Долгов А. Відповідальність за злочини, пов'язані з незаконним обігом крипто валют. *Ольвійський форум — 2025: стратегії країн Причорноморського регіону в геополітичному просторі* : мат-ли XXII Міжнар. наук. конф. (Миколаїв, 16—22.06.2025) / *Матеріали науково-практичних конференцій Чорноморського національного університету імені Петра Могили. Серія: Право.* 2025. № 1 (1). С. 40—43. DOI: 10.34132/mspc2025.01.11.08 (дата звернення: 08.04.2026).

10 Деревянко Б. В. Ризики здійснення операцій з криптовалютою (біткойнами) громадян і суб'єктів господарювання України. *Форум права*. 2017. № 3. С. 33—39. URL: https://repository.ndippp.gov.ua/bitstream/handle/765432198/269/Derevyanko__FP_2017_3_8.pdf?sequence=1&isAllowed=y (дата звернення: 07.05.2026).

11 Завидняк І. О. Особливості криміналістичної характеристики економічних транснаціональних злочинів, вчинених із використанням сучасних комп'ютерних технологій. *Аналітично-порівняльне правознавство*. 2021. № 3. С. 178—183. DOI: 10.24144/2788-6018.2021.03.33 (дата звернення: 08.04.2026).

12 Карчевський М. В., Шульженко Н. В., Куковинець Д. О. та ін. Міжнародні стандарти та національна кримінально-правова політика у сфері охорони інформаційної безпеки : монографія / за заг. ред. В. І. Борисова, М. В. Карчевського, М. В. Шепітька. Харків, 2023. 152 с. DOI: 10.31359/9789669986818 (дата звернення: 11.04.2026).

13 Малютін Е. В. Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу : автореф. дис. … канд. юрид. наук. Дніпро, 2024. 26 с. URL: https://dduvs.edu.ua/naukova-diyalnist/spetsializovani-vcheni-radi/ogoloshennya-pro-zahist-disertatsij/malyutin/ (дата звернення: 08.04.2026).

14 Неділько Я. В. Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій : дис. … д-ра філос. в галузі права. Київ, 2023. 257 с. URL: https://ir.library.knu.ua/server/api/core/bitstreams/902a977f-032e-4c47-84df-703ae2b1f64e/content (дата звернення: 08.04.2026).

15 Кремінський О. В. Розслідування легалізації (відмивання) доходів, отриманих злочинним шляхом, в умовах використання віртуальних валют : дис. … д-ра філос. в галузі права. Ірпінь, 2022. 229 с. URL: https://drive.google.com/file/d/1hRfh1Vp-mnRti_ftfs5eSfOSvhTI9rln/view (дата звернення: 08.04.2026).

16 Мовчан А. В., Козій В. В. Основи розслідування злочинів щодо незаконного заволодіння криптовалютою. *Наука і правоохорона*. 2022. № 4 (58). С. 178—189. DOI: 10.36486/np.2022.4(58).17 (дата звернення: 08.05.2026).

В. Сисолятіна [17] та ін. Питання міжнародно-правової регламентації інформаційної безпеки та формування національної кримінально-правової політики щодо цього розкрито у праці М. Карчевського зі співавторами. Зокрема, розглянуто питання інформаційної безпеки у сфері застосування інформаційних технологій у контексті користування ВА. Науковці запропонували науково-теоретичне визначення інформаційної безпеки, окреслили види суспільних відносин, що забезпечують її, висвітлили питання реалізації міжнародних стандартів протидії кримінальним правопорушенням у сфері застосування інформаційних технологій та обігу ВА [18].

У сучасних умовах глобальної цифровізації криптовалюти перетворюються на вагомий фінансовий інструмент, що завдяки анонімності та транскордонності кидає нові виклики економічній безпеці, включно з відмиванням коштів, фінансуванням тероризму та специфічними кіберзлочинами. Незважаючи на наявність міжнародних механізмів протидії та прийняття в Україні Закону «Про віртуальні активи» [19] (далі — *Закон про ВА*), правове регулювання залишається фрагментарним, а процес притягнення до відповідальності ускладнено анонімністю транзакцій, застосуванням міксерів, юрисдикційними колізіями та браком технічної експертизи у правоохоронних органів. А. Долгов визначив, що для подолання цих перешкод необхідна адаптація національного законодавства до міжнародних стандартів, системне підвищення цифрової компетентності слідчих і суддів, а також упровадження спеціалізованих інструментів моніторингу блокчейну, що дасть змогу ефективно інтегрувати ВА в офіційну фінансову систему за умови мінімізації кримінальних ризиків [20].

Останніми роками українська криміналістична наука помітно активізувала дослідження проблематики розслідування злочинів, пов'язаних з ВА. Прикладом є О. Кремінський, який сформував елементи криміналістичної характеристики легалізації (відмивання) доходів, отриманих злочинним шляхом, в умовах користування віртуальними валютами. Дослідник визначив, що криміналістична характеристика легалізації злочинних доходів із користуванням ВА базується на складних, заздалегідь спланованих схемах, які містять етапи підготовки, учинення й активного приховування слідів злочину за допомогою криптоказино (де відмивають до трьох чвертей коштів), анонімних передплачених карток, криптоматів та ігрових валют у *MMORPG*-іграх. Характерними ознаками таких злочинів є анонімність транзакцій, відсутність прив'язки рахунків до конкретних осіб і застосування сервісів-міксерів для заплутування ланцюжків блокчейну, що дає змогу суб'єктам з високим рівнем знань у сферах *IT* та фінансів ефективно маскувати джерела походження коштів (наркоторгівля, шахрайство, корупція).

17 Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук. Київ, 2024. 230 с. URL: https://uacademic.info/ua/document/0423U100236 (дата звернення: 08.04.2026).

18 Карчевський М. В., Шульженко Н. В., Куковинець Д. О. та ін. Зазнач твір. DOI: 10.31359/9789669986818 (дата звернення: 11.04.2026).

19 Про віртуальні активи : Закон України від 17.02.2022 р. № 2074-IX (зі змін. та допов.; не набрав чин.). URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text (дата звернення: 08.04.2026).

20 Долгов А. Зазнач твір. DOI: 10.34132/mspc2025.01.11.08 (дата звернення: 08.04.2026).

Процес розслідування значно ускладнює транскордонна природа операцій, де місцем злочину стає як локація комп'ютера, так і територія країни з обчислювальними потужностями, а доказова база часто формується не лише із цифрових слідів, а й із паперових чернеток. Типовий портрет правоохоронця-зловмисника — це ініціатори-одинаки, які діють у складі організованих груп, що керуються корисливими мотивами та користуються прогалинами в законодавстві й анонімністю криптосфери для уникнення відповідальності [21].

Окрему категорію становлять злочини, що скоюють із застосуванням інформаційних комп'ютерних технологій [22] і кримінальних правопорушень, пов'язаних із користуванням е-банкінгом [23]. Учені визначили основні елементи криміналістичної характеристики й механізми вчинення цих правопорушень, які є похідними для багатьох злочинів, пов'язаних з незаконним обігом ВА.

І. Завидняк сформувала в окремій праці особливості криміналістичної характеристики економічних транснаціональних злочинів, скоєних із застосуванням сучасних комп'ютерних технологій, які можна визначити як окрему категорію злочинів, пов'язаних з незаконним обігом ВА. Більшість із цих злочинів — зазвичай шахрайства, а за природою ВА вони мають саме транскордонний характер [24].

Важливими для становлення наукової думки щодо формування методів і методик протидії злочинам, пов'язаним з незаконним обігом ВА, є звіти, рекомендації та інша аналітична інформація українських і міжнародних органів, що протидіють кіберзлочинам, організованій злочинності й корупції, а також займаються фінансовим моніторингом з метою виявлення ознак легалізації (відмивання) коштів, здобутих злочинним шляхом.

Водночас у національному науковому середовищі немає наріжних і комплексних досліджень з визначення елементів криміналістичної характеристики кримінальних правопорушень, пов'язаних з незаконним обігом ВА. Зазначене обумовлює потребу в дослідженні цієї проблематики й висвітленні окремих її складників.

Викладення основного матеріалу дослідження

Основною метою криміналістичної характеристики є оптимізація процесу розкриття й розслідування злочину. Її можна уявити як ідеальну модель типових зв'язків і джерел доказової інформації, що дають змогу спрогнозувати оптимальний шлях і найбільш ефективні засоби розслідування окремих категорій злочинів [25].

21 Кремінський О. В. Зазнач твір. URL: https://drive.google.com/file/d/1hRfh1Vp-mnRti_ftfs5eSfOSvhTI9rln/view (дата звернення: 08.04.2026).

22 Неділько Я. В. Зазнач. твір. URL: https://ir.library.knu.ua/server/api/core/bitstreams/902a977f-032e-4c47-84df-703ae2b1f64e/content (дата звернення: 08.04.2026).

23 Малютін Е. В. Зазнач твір. URL: https://dduvs.edu.ua/naukova-diyalnist/spetsializovani-vcheni-radi/ogoloshennya-pro-zahist-disertatsij/malyutin/ (дата звернення: 08.04.2026) ; Сисолятін В. В. Зазнач. твір. URL: https://uacademic.info/ua/document/0423U100236 (дата звернення: 08.04.2026).

24 Завидняк І. О. Зазнач. твір. DOI: 10.24144/2788-6018.2021.03.33 (дата звернення: 08.04.2026).

25 Батюк О. В., Благута Р. І., Гумін О. М. та ін. Методика розслідування окремих видів злочинів, підслідних органам внутрішніх справ : навч. посіб. / за заг. ред. Є. В. Пряхіна. Львів, 2011. 324 с.

Першим важливим елементом криміналістичної характеристики І. Завидняк називає предмет злочинних посягань, оскільки він має безпосередній вплив на інші елементи та є умовою певних способів скоєння та приховування злочину, ознак особи злочинця (злочинів) [26]. На нашу думку, це твердження цілком слушне, оскільки в нашому випадку особливий предмет — ВА — створює унікальні кореляційні зв'язки. Варто погодитися з тим, що залишити такі сліди, як публічні ключі гаманців, кількість переказаних ВА, унікальний хеш транзакції, точний час переказу й суму комісії, може винятково криптовалюта.

Оскільки ВА за своєю суттю є специфічними масивами даних, особливого значення набуває аналіз природи комп'ютерної інформації як їхнього змістовного базису. Попри те, що кримінальне процесуальне законодавство України сьогодні не виокремлює цифрових даних в індивідуальну категорію доказової бази, під час розслідування відповідних злочинів головну роль відіграють інформаційні сліди, які після належного юридичного оформлення трансформуються в повноцінні докази. Слід наголосити на віртуальній природі комп'ютерної інформації, яка позбавлена традиційного матеріального втілення і стає доступною для аналізу лише за допомогою застосування програмно-технічних засобів, що перетворюють цифрові коди на форму, зрозумілу для людського сприйняття. У широкому розумінні таку інформацію можна визначити як сукупність відомостей, які існують на електронних накопичувачах або які передають мережевими каналами, підлягають обробленню, модифікації та відтворенню за допомогою обчислювальних систем і телекомунікаційних мереж [27].

Правова природа ВА в Україні, навіть без набрання чинності Законом про ВА, перебуває у площині легальних правовідносин, оскільки згідно зі ст. 177 Цивільного кодексу України (далі — *ЦК України*):

«1. Об'єктами цивільних прав є речі, гроші, цінні папери, цифрові речі, майнові права, роботи та послуги, результати інтелектуальної, творчої діяльності, інформація, а також інші матеріальні та нематеріальні блага.

2. Об'єкти цивільних прав можуть існувати у матеріальному світі та/або цифровому середовищі, що обумовлює форму об'єктів, особливості набуття, здійснення та припинення цивільних прав і обов'язків щодо них» [28].

До того ж відповідно до ст. 179-1 ЦК України ВА є цифровою річчю [29], і в судів не виникає питань із захистом прав потерпілих у разі заволодіння їхнім майном у вигляді ВА.

Якщо розглядати як предмет злочину найпоширеніші ВА — криптовалюти,— то поміж них найпомітніше місце посідають конвертовані валюти, які мають еквівалентну вартість у фіатній валюті й можуть бути обміняні на звичайні гроші. У сучасній класифікації цифрових активів до них належать *Bitcoin* і *E-Gold*. Неконвертовані валюти зазвичай обмежені екосистемою конкретного програмного продукту. Вони за своєю природою подібні до віртуальних гро-

26 Завидняк І. О. Зазнач твір. DOI: 10.24144/2788-6018.2021.03.33 (дата звернення: 08.04.2026).

27 Мазуренко О., Розенфельд Н. Комп'ютерна інформація як предмет правопорушень, передбачених Розділом XVI КК України. *Право України*. 2004. Т. 6. С. 80—83.

28 Цивільний кодекс України від 16.01.2003 р. № 435-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 08.04.2026).

29 Там само.

шей у відеоіграх; за відсутності об'єктивної ринкової ціни вони рідко стають об'єктом інтересу правопорушників. Проте існують механізми перетворення таких закритих систем на відкриті за допомогою неофіційних каналів обміну, що де-факто робить їх конвертованими всупереч правилам розробників [30].

Однією з об'єктивних умов учинення кримінальних правопорушень, пов'язаних з незаконним обігом ВА, які зазвичай скоюють транснаціональні об'єднані злочинні угруповання, є чітка детермінація такого виду злочинів об'єктивною обстановкою у світі та в законодавстві багатьох країн [31].

Як зазначає Я. Неділько, у структурі обстановки таких кримінальних правопорушень, з огляду на їх особливості, слід виокремлювати: кіберпростір, що характеризується місцем, часом, віртуальною взаємодією учасників кримінального правопорушення; матеріальне середовище — ділянку території, сукупність різних предметів, поведінку учасників події, психологічні взаємини [32].

Обстановка правопорушення як комплекс матеріальних елементів у місці події дає змогу реконструювати алгоритм злочинного акту і специфіку поведінки його суб'єктів. Злочини в досліджуваній сфері відзначаються винятковим рівнем інтелектуальної підготовки й застосуванням багаторівневих методів опосередкованого впливу на цифрові системи, що суттєво ускладнює фіксування фактів несанкціонованого доступу. Характерною ознакою таких діянь є територіальна роз'єднаність: локація, де безпосередньо реалізовано злочинний задум (активні дії), зазвичай географічно не збігається з місцем виникнення суспільно небезпечних наслідків. Зважаючи на транскордонну природу кіберзлочинів і труднощі (а подекуди й неможливість) ідентифікації фізичної точки, з якої здійснено втручання, у криміналістичній і судовій практиці доцільно вважати місцем скоєння злочину ту територію, де фактично настали шкідливі результати протиправної діяльності [33].

Е. Малютін визначив і схарактеризував місця учинення злочинних дій, пов'язаних з користуванням е-банкінгом, співвідносних з кіберзлочинами з незаконного заволодіння ВА: місця розміщення пристроїв, якими скористалися для вчинення протиправних дій (смартфон, комп'ютер, ноутбук, планшет) — 74 %; місця розташування банкоматів, банків, а також інших закладів фінансової сфери — 16 %; місце перебування потерпілої особи, на яку були спрямовані протиправні дії,— 9 % [34].

Часові обставини є визначеними особливостями скоєння злочину в певний час доби, у певні дні, місяці й роки. Скоєння злочинів, які розглядаємо, зазвичай розпочинається з неправомірного доступу до інформації. Останній здійснюють під час роботи комп'ютера, він не обмежений певним часовим

30 Громек М. Розшифровка криптозлочинів : посіб. для правоохорон. орган. / OSCE : web. 2024. 64 с. URL: https://oceea.osce.org/sites/default/files/f/documents/b/c/601719.pdf (дата звернення: 08.04.2026).

31 Цивільний кодекс України … . URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 08.04.2026).

32 Неділько Я. В. Зазнач. твір. URL: https://ir.library.knu.ua/server/api/core/bitstreams/902a977f-032e-4c47-84df-703ae2b1f64e/content (дата звернення: 08.04.2026).

33 Завидняк І. О. Зазнач. твір. DOI: 10.24144/2788-6018.2021.03.33 (дата звернення: 08.04.2026).

34 Малютін Е. В. Зазнач. твір. URL: https://dduvs.edu.ua/naukova-diyalnist/spetsializovani-vcheni-radi/ogoloshennya-pro-zahist-disertatsij/malyutin/ (дата звернення: 08.04.2026).

проміжком, оскільки автоматизовані інформаційні системи можуть функціювати цілодобово [35]. Проте кожен спосіб скоєння таких злочинів, пов'язаний із застосуванням сучасних комп'ютерних технологій, має певні часові особливості, оскільки зазвичай має місце різниця в часі, і в разі вчинення такого кримінальні правопорушення вночі можна припускати, що зловмисники діють в іншому часовому поясі, де в цей час день.

Щодо способів підготовки до скоєння злочинів досліджуваного виду, то можна виокремити такі: виготовлення шпигунських технічних або програмних засобів для протиправного застосування під час здійснення операцій з викрадення ВА; збут або поширення без необхідного дозволу в інтернеті відомостей, які мають значення під час здійснення операцій з ВА; створення сайтів з відповідною тематикою для шахрайських схем (псевдобіржі, псевдообмінні сервіси, сайти знайомств тощо) [36].

Існує велика кількість способів скоєння злочинів, пов'язаних з незаконним обігом ВА, тому в межах цієї праці ми розглянемо кілька позицій науковців із зазначеної тематики й найбільш поширені способи, якими послуговуються злочинці всього світу.

За А. Долговим, до способів учинення шахрайства із застосуванням ВА належать такі явища: *rug pull* (раптове зникнення ліквідності, тобто штучне накручування ціни криптоактиву з наступним його обвалом через продаж його основної маси), *NFT*-шахрайство (підробка, плагіат унікальних ВА) і *DeFi*-експлойти (застосування вразливостей протоколів для зламу цифрових сервісів і крадіжки ВА) [37].

Б. Деревянко розглядає такі два способи вчинення шахрайства із ВА: викрадення відомостей про *ID*-гаманець і пароль від нього; незаконне передавання третім особам інформації про *ID*-гаманець і пароля власника біткойнів самою фірмою-надавачем послуг з розміщення гаманця. Хоча на своїх сайтах і в договорі такі сервіси зазначають, що не цікавляться паролем власника криптовалюти, усе одно існують серйозні сумніви щодо цього. І беззаперечним правовим ризиком є ризик зміни в односторонньому порядку надавачем послуг з розміщення електронного гаманця умов договору та/або запровадження платних послуг [38].

А. Мовчан і В. Козій виокремлюють такі способи вчинення кримінальних правопорушень, пов'язаних з незаконним обігом криптоактивів:

1) злам криптовалютних бірж та електронних гаманців фізичних осіб і виведення криптовалюти на біржі, обмінні ресурси або інші електронні гаманці;
2) інсценування викрадення криптовалюти самими біржами;
3) шахрайські дії:
   - добровільне передавання потерпілим активів на фіктивні сервіси, контрольовані зловмисниками. Наслідком є повна втрата доступу до ресурсів: або через програмні маніпуляції, які відо-

35 Панов М. І., Шепітько В. Ю., Коновалова В. О. та ін. Настільна книга слідчого : наук.-практ. вид. для слідч. і дізнавач. 2-ге вид., перероб. і допов. Київ, 2007. 728 с.

36 Малютін Е. В. Зазнач. твір. URL: https://dduvs.edu.ua/naukova-diyalnist/spetsializovani-vcheni-radi/ogoloshennya-pro-zahist-disertatsij/malyutin/ (дата звернення: 08.04.2026).

37 Долгов А. Зазнач твір. DOI: 10.34132/mspc2025.01.11.08 (дата звернення: 08.04.2026).

38 Деревянко Б. В. Зазнач. твір. URL: https://repository.ndippp.gov.ua/bitstream/handle/765432198/269/Derevyanko__FP_2017_3_8.pdf?sequence=1&isAllowed=y (дата звернення: 07.05.2026).

бражають нульовий баланс у кабінеті користувача, або внаслідок раптового припинення діяльності сервісу (*exit scam*), коли оператори зникають разом із довіреними їм активами;

- викрадення конфіденційної інформації через фішингові атаки. Це метод інтернет-шахрайства, спрямований на отримання несанкціонованого доступу до облікових записів на криптобіржах або приватних ключів електронних гаманців, через спонукання жертв перейти на підроблену сторінку та ввести логін і пароль, що дає їм змогу миттєво спустошити баланс;
- маніпулятивні схеми типу *Scam* (у перекл. з англ. *афера або шахрайство*). Суть полягає у випуску на ринок нового токена, вартість якого організатори штучно збільшують. Укладаючи значні ресурси в маркетинговий хайп у соцмережах та імітуючи бурхливе зростання ціни, шахраї залучають масу дрібних інвесторів. Коли вартість активу сягає пікових значень, організатори масово розпродають власні запаси, отримуючи надприбутки. Як наслідок, ціна миттєво обвалюється, а вкладники залишаються з неліквідними цифровими одиницями, які не мають реальної вартості;
- випуск імітаційних токенів (клонів). Правопорушники створюють цифрову монету, назва якої цілком копіює або максимально подібна до назви перспективного проєкту, що ще не пройшов лістинг на великих біржах. Активно рекламуючи такий «аналог» у месенджерах і соціальних групах, шахраї наводять посилання на власні смарт-контракти: інвестори помилково купують фальсифікат, який не має жодного стосунку до реального проєкту й не може бути реалізований на ринку [39].

За даними *Chainalysis* (*2026 Crypto Crime Report*), найбільш популярними способами кримінальних правопорушень, пов'язаних з незаконним обігом ВА, є шахрайство, як-от:

1) фішингові клони обмінників. Шахраї створюють копії сайтів відомих обмінників. Зовні сторінки виглядають майже ідентично завдяки тому самому дизайну, формі заявки та курсу (домен відрізняється одним символом; відсутні офіційні контакти або правила обміну; пропозиція «найкращий курс тільки сьогодні»);
2) підміна реквізитів у листуванні. Обмін погоджують у чаті або месенджері, після чого співрозмовник раптово повідомляє, що реквізити змінилися (реквізити змінюються в останній момент; співрозмовник просить перейти в інший чат або контакт; дані надсилають зображенням, а не текстом). Це може виглядати буденно, наприклад, «вибачте, попередній гаманець тимчасово не працює», «скористайтеся іншим рахунком» тощо. Якщо користувач не перевіряє деталей, криптовалюта потрапляє на адресу шахрая;
3) фейкове підтвердження платежу. Після домовленості про обмін шахрай надсилає скрин нібито проведеної оплати. Далі починається

39 Мовчан А. В., Козій В. В. Зазнач. твір. DOI: 10.36486/np.2022.4(58).17 (дата звернення: 08.05.2026).

тиск, мовляв, гроші вже відправлені, тому потрібно негайно перевести криптовалюту й не очікувати надходження;

4) підміна *QR*-коду або адреси гаманця. Користувачеві надсилають *QR*-код або адресу для переказу криптовалюти. Насправді вони ведуть на гаманець шахрая. Таке стається, коли адреси копіюють через сторонні сервіси або отримують у чатах без перевірки (просять установити «спеціальне» розширення або програму; пропонують підключитися через віддалений доступ; адреса виглядає незнайомою або відрізняється від попередньо погодженої);
5) маніпулювання курсом після заявки. Спочатку пропонують курс, який виглядає трохи вигіднішим за ринковий. Коли користувач уже відправив криптовалюту, з'являються додаткові умови. Часто це додаткова комісія за перевірку, плата за прискорення, новий курс. У підсумку отримана сума значно менша, аніж очікувалося;
6) фейкова служба підтримки. Шахраї представляються співробітниками сервісу або модераторами платформи. Вони пишуть користувачеві й повідомляють про нібито проблему з транзакцією. Далі намагаються отримати доступ до гаманця, просять *seed*-фразу, коди *2FA*, доступ до пристрою або гаманця;
7) фальшивий гарант. У *Telegram* або іншому чаті пропонують провести обмін за допомогою гаранта, який нібито контролюватиме угоду та триматиме кошти до завершення операції. Насправді гарант може бути частиною шахрайської схеми. Він наполягає на швидкому проведенні операції і не має підтвердженої репутації за межами цього діалогу;
8) підміна мережі або токена. Користувача просять відправити криптовалюту через іншу мережу або на інший токен. Наприклад, замість *USDT TRC20* пропонують *USDT ERC20* або надсилають реквізити для *USDT* у мережі, яку гаманець користувача не підтримує. У результаті кошти можуть «зависнути» або їх буде складно повернути. Мережа змінюється просто під час угоди, а пояснення виглядає поспішним або нечітким;
9) ризики готівкового обміну. Обмін проводять під час особистої зустрічі. Проблеми виникають у момент передавання грошей, де можливі недовкладення, підміна купюр або інші маніпуляції (зустріч призначають у випадковому місці; намагаються прискорити передавання грошей; заважають спокійно перерахувати й перевірити купюри);
10) фейкова *AML*-перевірка. Після отримання криптовалюти користувачеві повідомляють, що кошти нібито потрапили під *AML*-перевірку, й вимагають додатковий платіж, який виправдовують обов'язковою заставою, податком або комісією за перевірку й обіцяють, що після цього транзакцію розблокують. Головна ознака — вимога доплати та відсутність заздалегідь відомого регламенту перевірки [40].

40 10 схем шахрайства при обміні криптовалюти у 2026 році: як розпізнати та захиститися / Finance.ua : вебсайт. 25.03.2026. URL: https://finance.ua/ua/goodtoknow/10-skhem-shakhraistva-pry-obmini-kryptovaliuty-u-2026-rotsi-yak-rozpiznaty-ta-zakhystytysia (дата звернення: 08.04.2026).

Ми пропонуємо об'єднати способи вчинення таких кримінальних правопорушень у групи: *«оцифровані» злочини*, пов'язані з незаконним обігом ВА (скоєні винятково із застосуванням кібернетичних методів) і *класичні злочини* (наприклад, викрадення людини з подальшим вимаганням викупу у вигляді ВА, умисне вбивство з метою заволодіти ВА потерпілого тощо).

Щодо способів відмивання майна, то майже всі транскордонні організовані злочинні угруповання відмивають кошти із користуванням ВА й офшорними юрисдикціями, що є найпоширенішими способами на завершальній фазі, пов'язаній з ухиленням від оподаткування та приховуванням слідів. Як зазначає В. Божик, у 87 % кримінальних проваджень усе відбувається за такою схемою: офшор, фіктивне підприємництво («конвертаційні центри»), формування схемного податкового кредиту, порушення митних правил і контрабанда, контрафакт, виведення прибутку через псевдопідприємництво фізичних осіб, фізична особа, заниження оборотів [41].

Новим і популярним способом легалізації кримінальних доходів є їх відмивання за допомогою сайтів азартних ігор. Саме через ці сервіси відмивають майже три чверті всіх брудних віртуальних грошей. Згідно з даними *Trend Micro*, злочинці дедалі частіше звертаються до ігрової валюти як способу зберігання вартості криптовалюти. Для цього за криптовалюту купують валюту найбільш популярних віртуальних ігор, а потім на спеціальних сервісах конвертації обмінюють її на фіатну валюту [42].

Іще одним способом приховування кримінальних правопорушень, пов'язаних з незаконним обігом ВА, є користування децентралізованими біржами, позабіржовими біржами (так званими *OTC*-угодами, від англ. *Over-the-Counter* — поза прилавком), міксерами й тумблерами. Цю технологію розробили для приховування слідів транзакцій користувачів. Багато держав — учасниць ОБСЄ вживають заходів для обмеження використання таких інструментів. Міксери та тумблери — це послуги, призначені для підвищення конфіденційності й анонімності криптовалютних транзакцій. Їхня основна функція полягає в змішуванні коштів різних користувачів, що маскує джерело походження коштів [43].

Особи злочинців у досліджуваному виді злочинів умовно можна об'єднати в три групи. Першу групу становлять особи, які поєднують високий рівень професійної підготовки у сфері інформаційних технологій і програмування з нестандартним мисленням, технічною винахідливістю та певною схильністю до професійного азарту. Для них комп'ютерні системи — не лише інструмент для роботи, а й середовище для реалізації власних інтелектуальних можливостей. До цієї групи можуть належати працівники криптовалютних бірж, майнінгових підприємств, компаній-емітентів ВА, а також спеціалісти технічних компаній, що забезпечують відповідні структури хмарними, штучно-інтелектуальними й іншими цифровими сервісами.

До другої групи належать професійні кіберзлочинці, діяльність яких має чітко виражений корисливий характер.

41 Божик В. І. Зазнач твір. DOI: 10.24144/2307-3322.2026.93.5.3 (дата звернення: 08.04.2026).

42 Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing : FATF Report / FATF : web. Sept. 2020. 24 p. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf.coredownload.pdf (дата звернення: 07.05.2026).

43 Громек М. Зазнач. твір. URL: https://oceea.osce.org/sites/default/files/f/documents/b/c/601719.pdf (дата звернення: 08.04.2026).

Саме ця категорія становить одну з найбільших загроз як для окремих суб'єктів господарювання, так і для міжнародної економічної безпеки загалом. Представники цієї групи часто формують ядро транснаціональних злочинних угруповань, які послуговуються сучасними інформаційними технологіями для вчинення економічних правопорушень у значних масштабах.

Третя група — це так звані респектабельні правопорушники: особи, які мають легальний професійний статус і спеціальні знання у сфері фінансів, обліку або програмування. До них можуть належати бухгалтери, економісти та програмісти, які застосовують свої професійні навички для підготовки й реалізації злочинних схем, орієнтованих переважно на отримання матеріальної вигоди [44].

Наголосимо, що економічні транснаціональні злочини із застосуванням сучасних комп'ютерних технологій зазвичай скоюють організовані злочинні угруповання. Саме тому осіб, які їх скоїли, запропоновано досліджувати *«за схемою: 1) загальні особливості злочинця, який вчинив економічний транснаціональний злочин, із використанням комп'ютерних технологій та 2) особливості осіб, які вчинили певні різновиди таких злочинів, з урахуванням розподілу ролей в організованій злочинній групі»* [45].

Найбільш поширеним мотивом скоєння злочинів цієї категорії є корисливі міркування, дуже рідко — помста. Особи, здатні таке зробити, є серйозною загрозою для економіки будь-якої держави й міжнародної спільноти загалом [46].

Найголовніші первинні сліди злочинів, пов'язаних з незаконним обігом ВА, містяться у блокчейні. До відкритих відомостей належать: адреси відправника й одержувача (публічні ключі гаманців), сума переказу (кількість токенів або криптовалюти), хеш транзакції (унікальний ідентифікатор, за яким можна знайти запис), часова мітка (точний час підтвердження транзакції), комісія. Ці сліди матимуть місце в разі використання звичайної криптовалюти, однак існують анонімні коїни (*monero, zcash, dash, xeonbit*), які складно відстежити, оскільки вони послуговуються специфічною модифікацією блокчейну, спрямованою на забезпечення анонімності й конфіденційності транзакцій.

Узагальнюючи викладене, слід наголосити, що для таких кримінальних правопорушень типовою ознакою є наявність цифрових або електронних слідів, які виникають у процесі застосування інформаційних технологій. Подібну інформацію можуть містити облікові записи користувачів, пам'ять комп'ютерної техніки й інших електронних пристроїв, профілі в соціальних мережах, ресурси для спілкування або обміну інформацією щодо криптовалют, бази даних операторів телекомунікацій та інтернет-провайдерів, а також змінні носії інформації, зокрема *USB*-накопичувачі [47].

Якщо потерпілий контактував з правопорушником особисто або за допомогою відеозв'язку, він може надати інформацію про зовнішні ознаки й інші характеристики особи злочинця [48]. На жаль, найчастіше потерпілий не має

44 Завидняк І. О. Зазнач. твір. DOI: 10.24144/2788-6018.2021.03.33 (дата звернення: 08.04.2026).
45 Там само.
46 Там само.
47 Сисолятін В. В. Зазнач. твір. URL: https://uacademic.info/ua/document/0423U100236 (дата звернення: 08.04.2026).
48 Малютін Е. В. Зазнач. твір. URL: https://dduvs.edu.ua/naukova-diyalnist/spetsializovani-vcheni-radi/ogoloshennya-pro-zahist-disertatsij/malyutin/ (дата звернення: 08.04.2026).

візуального контакту з правопорушником [49].

Висновки

Проведене дослідження дало змогу розкрити основні елементи криміналістичної характеристики кримінальних правопорушень, пов'язаних з незаконним обігом ВА, і визначити їх специфічні особливості в умовах сучасної цифровізації суспільства. З'ясовано, що ВА як предмет злочинного посягання формують особливий механізм злочинної діяльності, який характеризується застосуванням інформаційних технологій, транскордонністю операцій, високим рівнем латентності та складністю виявлення й документування доказової інформації.

Визначено, що основним джерелом доказової інформації в таких кримінальних правопорушеннях є цифрові сліди, які можуть міститися у блокчейні, електронних гаманцях, акаунтах користувачів, пам'яті комп'ютерної техніки, месенджерах, соціальних мережах, базах даних операторів зв'язку й інтернет-провайдерів. Водночас особливості функціювання анонімних криптовалют, міксерів, тумблерів і децентралізованих платформ суттєво ускладнюють процес установлення джерела походження активів і маршруту їх переміщення.

У результаті аналізу способів учинення досліджуваних кримінальних правопорушень з'ясовано, що найбільш поширеними є різноманітні форми шахрайства, фішингові атаки, злам криптовалютних бірж та електронних гаманців, маніпуляції з токенами, користування фіктивними платформами й сервісами, а також легалізація доходів через криптовалютні сервіси, онлайн-казино й офшорні юрисдикції. Визначено, що злочинну діяльність у цій сфері часто здійснюють організовані транснаціональні угруповання з чітким розподілом ролей між учасниками.

Дослідження особи правопорушника дало змогу виокремити кілька типових категорій суб'єктів таких злочинів: технічно підготовлених спеціалістів у сфері ІТ, професійних кіберзлочинців та осіб з легальним професійним статусом, які застосовують спеціальні знання у фінансовій або технічній сфері для реалізації злочинних схем. Спільною ознакою більшості правопорушників є високий рівень цифрової компетентності й орієнтування на отримання матеріальної вигоди.

Отже, кримінальні правопорушення, пов'язані з незаконним обігом ВА, є складним багаторівневим явищем, що поєднує елементи кіберзлочинності, економічної злочинності та транснаціональної організованої діяльності. Це обумовлює потребу в подальшому розвитку криміналістичних методик їх виявлення та розслідування, удосконаленні законодавчого регулювання у сфері обігу ВА, а також у підвищенні рівня технічної підготовки правоохоронних органів щодо роботи із цифровими доказами та технологіями блокчейну.

Forensic Characteristics of Criminal Offenses Related to Illegal Circulation of Virtual Assets

Dmytro Nesterov

This article purpose is to reveal peculiarities of forensic characteristics of crimes related to illegal circulation of virtual assets, as well as to determine the main elements of their commission mechanism. For achieving this goal, complex of general scientific and special legal

49 Сисолятін В. В. Зазнач. твір. URL: https://uacademic.info/ua/document/0423U100236 (дата звернення: 08.04.2026).

methods of cognition was applied, in particular dialectical, system-structural, formal-legal, comparative-legal, logical-semantic one, analysis and synthesis, modeling and generalization. The article is devoted to research on forensic characteristics of criminal offenses related to illegal circulation of virtual assets, which in conditions of global digitalization and rapid information development of technologies are becoming increasingly dangerous to society. Topic relevance is due to active use of cryptocurrencies, decentralized financial services, anonymous payment instruments and artificial intelligence technologies in mechanisms of committing fraud, cybercrime and legalization of proceeds from crime. Growth of transnational cybercrime, spread of phishing schemes, use of mixers, toggle switches, offshore jurisdictions and platforms with end-to-end encryption create significant difficulties for law enforcement agencies in detecting, documenting and investigating such offenses. Particular attention is paid to the problems of forming an evidentiary base associated with virtual nature of digital traces and difficulty of identifying persons involved in illegal transactions with virtual assets. The research results determined that virtual assets as a subject of criminal encroachment form specific mechanism of criminal activity that is characterized by a high level of latency, cross-border nature, use of modern information technologies and complexity of localizing the place of commission of a criminal offense. It was substantiated that digital traces contained in blockchain, electronic wallets, user accounts, PC memory, messengers, social networks, databases of communication operators and Internet providers are of crucial importance for the investigation. The most common methods of committing crimes related to the illegal circulation of virtual assets are analyzed, including phishing attacks, hacking of cryptocurrency exchanges and electronic wallets, use of fake platforms, manipulation of tokens, fraudulent investment projects, DeFi-exploits, NFT fraud and legalization of income using cryptocurrency services and online casinos. It is proven that significant part of such offenses is committed by transnational organized criminal groups with a clear division of roles between participants. It is argued that offender in this category of crimes is characterized by a high level of digital competence, specific expertise in the field of information technology, programming or finance and an orientation towards obtaining material benefits. It is proposed to classify the subjects of such criminal offenses as technically trained specialists, professional cybercriminals and persons with legal professional status who apply their knowledge to implement criminal schemes. It is concluded that criminal offenses related to illegal circulation of virtual assets are a complex multi-level phenomenon that combines cybercrime peculiarities, economic crime and transnational organized activity. The need for further development of forensic investigation methods, improvement of legislative regulation of circulation of virtual assets and increasing level of technical training of law enforcement agencies in the field of work with digital evidence and blockchain technologies is emphasized.

Keywords: *virtual asset; blockchain; cross-border crimes; legalization (laundering) of money obtained by criminal means; fraud; theft; forensic characteristics; illicit trafficking.*

Фінансування

Це дослідження не отримало жодного спеціального гранту від фінансових установ у державному, комерційному або некомерційному секторах.

Відмова від відповідальності

Засновники не грали жодної ролі у розробленні дослідження, добиранні й аналізуванні даних, рішенні про публікацію або підготовку рукопису.

Учасники

Автор зробив свій внесок винятково в інтелектуальну дискусію, що є основою цього документа, дослідження судової

практики, написання та редагування, і бере на себе відповідальність за її зміст і тлумачення.

Декларація щодо конфлікту інтересів

Автор заявляє, що у нього відсутній конфлікт інтересів.

References

10 skhem shakhraistva pry obmini kryptovaliuty u 2026 rotsi: yak rozpiznaty ta zakhystytysia [10 Cryptocurrency Exchange Scams in 2026: How to Recognize and Protect Yourself] (2026) / Finance.ua : vebsait. 25.03. URL: https://finance.ua/ua/goodtoknow/10-skhem-shakhraistva-pry-obmini-kryptovaliuty-u-2026-rotsi-yak-rozpiznaty-ta-zakhystytysia [in Ukrainian].

Batiuk, O. V., Blahuta, R. I., Humin, O. M. ta in. (2011). *Metodyka rozsliduvannia okremykh vydiv zlochyniv, pidslidnykh orhanam vnutrishnikh sprav* [Methods for investigating certain types of crimes under investigation by internal affairs bodies] : navch. posib. / za zah. red. Ye. V. Priakhina. Lviv [in Ukrainian].

Bozhyk, V. I. (2026). Kryminalistychna kharakterystyka lehalizatsii maina, oderzhanoho vnaslidok ukhylennia vid splaty podatkiv: elementy ta mekhanizm zlochynnoi diialnosti [Forensic characteristics of property laundering resulting from tax evasion: structural elements and mechanisms of criminal activity]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia: Pavo*. Vyp. 93. Ch. 5. DOI: 10.24144/2307-3322.2026.93.5.3 [in Ukrainian].

Crypto Crime in 2025 Was Primarily Driven by 694% Surge in State-Driven Sanctions Evasion Volume (2026) / Chainalysis : web. March 5. URL: https://live-chainalysis.pantheonsite.io/blog/crypto-sanctions-2026/.

Cyber-Enabled Fraud. Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks. February 2026 (2026) / FATF : web. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Cyber-Enabled-Fraud%E2%80%93Digitalisation-and-ML-TF-PF-Risks.pdf.coredownload.inline.pdf.

Derevianko, B. V. (2017). Ryzyky zdiisnennia operatsii z kryptovaliutoiu (bitkoinamy) hromadian i sub'iektiv hospodariuvannia Ukrainy [Risks of Operations with Cryptocurrency (Bitcoins) for Citizens and Economic Entities of Ukraine]. *Forum prava*. № 3. URL: https://repository.ndippp.gov.ua/bitstream/handle/765432198/269/Derevyanko__FP_2017_3_8.pdf?sequence=1&isAllowed=y [in Ukrainian].

Dolhov, A. (2025). Vidpovidalnist za zlochyny, pov'iazani z nezakonnym obihom krypto valiut [Liability for crimes related to the illicit trafficking of cryptocurrencies]. Olviiskyi forum — 2025: stratehii krain Prychornomorskoho rehionu v heopolitychnomu prostori : mat-ly XXII Mizhnar. nauk. konf. (Mykolaiv, 16—22.06.2025) / *Materialy naukovo-praktychnykh konferentsii Chornomorskoho natsionalnoho universytetu imeni Petra Mohyly. Seriia: Pravo*. № 1 (1). DOI: 10.34132/mspc2025.01.11.08 [in Ukrainian].

Hromek, M. (2024). *Rozshyfrovka kryptozlochyniv* [Decrypting cryptocrimes] : posib. dlia pravookhoron. orhan. / OSCE : web. URL: https://oceea.osce.org/sites/default/files/f/documents/b/c/601719.pdf [in Ukrainian].

IOCTA 2026 – The evolving threat landscape: how encryption, proxies and AI are expanding cybercrime. Internet Organised Crime Threat Assessment (IOCTA) 2026 (2026) / EUROPOL : web. 28 Apr. DOI: 10.2813/5737847.

Karchevskyi, M. V., Shulzhenko, N. V., Kukovynets, D. O. ta in. (2023). *Mizhnarodni standarty ta natsionalna kryminalno-pravova polityka u sferi okhorony informatsiinoi bezpeky* [International standards and national criminal law policy in the field of information security protection] : monohrafiia / za zah. red. V. I. Borysova, M. V. Karchevskoho, M. V. Shepitka. Kharkiv. DOI: 10.31359/9789669986818 [in Ukrainian].

Kreminskyi, O. V. (2022). *Rozsliduvannia lehalizatsii (vidmyvannia) dokhodiv, otrymanykh zlochynnym shliakhom, v umovakh vykorystannia virtualnykh valiut* [Investigation of legalization (laundering) of criminal income by use virtual currencies] : dys. … d-ra filos. v haluzi prava. Irpin. URL: https://drive.google.com/file/d/1hRfh1Vp-mnRti_ftfs5eSfOSvhTI9rln/view [in Ukrainian].

Maliutin, E. V. (2024). *Osnovy metodyky rozsliduvannia kryminalnykh pravoporushen, pov'iazanykh iz vykorystanniam e-bankinhu* [Basics of the methodology of investigation of criminal offenses related to the use of e-banking] : avtoref. dys. … kand. yuryd. nauk. Dnipro. URL: https://dduvs.edu.ua/naukova-diyalnist/spetsializovani-vcheni-radi/ogoloshennya-pro-zahist-disertatsij/malyutin/ [in Ukrainian].

Mazurenko, O., Rozenfeld, N. (2004). Komp'iuterna informatsiia yak predmet pravoporushen, peredbachenykh Rozdilom XVI KK Ukrainy [Computer information as the subject of offenses provided for in Chapter XVI of Criminal Code of Ukraine]. *Pravo Ukrainy*. T. 6 [in Ukrainian].

Movchan, A. V., Kozii, V. V. (2022). Osnovy rozsliduvannia zlochyniv shchodo nezakonnoho zavolodinnia kryptovaliutoiu [Fundamentals of investigation crimes regarding illegal possession of cryptocurrency]. *Nauka i pravookhorona*. № 4 (58). DOI: 10.36486/np.2022.4(58).17 [in Ukrainian].

Nedilko, Ya. V. (2023). *Rozsliduvannia kryminalnykh pravoporushen, shcho vchyniaiutsia z vykorystanniam informatsiinykh komp'iuternykh tekhnolohii* [Investigation of criminal offenses committed using information computer technologies] : dys. … d-ra filos. v haluzi prava. Kyiv. URL: https://ir.library.knu.ua/server/api/core/bitstreams/902a977f-032e-4c47-84df-703ae2b1f64e/content [in Ukrainian].

Panov, M. I., Shepitko, V. Yu., Konovalova, V. O. ta in. (2007). *Nastilna knyha slidchoho* [The Handbook for an Investigator] : nauk.-prakt. vyd. dlia slidch. i diznavach. 2-he vyd., pererob. i dopov. Kyiv [in Ukrainian].

Shchorichnyi zvit Departamentu kiberpolitsii Natsionalnoi politsii Ukrainy za 2025 rik [Annual report of the Cyber Police Department of National Police of Ukraine for 2025] (2026) / Kiberpolitsiia Ukrainy : ofits. vebsait. 16.02. URL: https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/ [in Ukrainian].

Sysoliatin, V. V. (2024). *Rozsliduvannia kryminalnykh pravoporushen, pov'iazanykh iz vykorystanniam internet-bankinhu* [Investigation of criminal offenses related with the using of Internet banking] : dys. … kand. yuryd. nauk. Kyiv. URL: https://uacademic.info/ua/document/0423U100236 [in Ukrainian].

Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (2020) : FATF Report / FATF : web. Sept. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf.coredownload.pdf.

Zavydniak, I. O. (2021). Osoblyvosti kryminalistychnoi kharakterystyky ekonomichnykh transnatsionalnykh zlochyniv, vchynenykh iz vykorystanniam suchasnykh komp'iuternykh tekhnolohii [Features of the criminalistic characteristics of economic transnational crimes committed with the use of modern computer technologies]. *Analitychno-porivnialne pravoznavstvo*. № 3. DOI: 10.24144/2788-6018.2021.03.33 [in Ukrainian].

Нестеров, Д. (2026). Криміналістична характеристика кримінальних правопорушень, пов'язаних з незаконним обігом віртуальних активів. *Теорія та практика судової експертизи і криміналістики*. Вип. 2 (43). С. 184—202. DOI: 10.32353/khrife.2.2026.12.