

КРИМІНАЛЬНЕ ПРАВО ТА ПРОЦЕС; КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 343.9::004.9:336.74

DOI: 10.36550/2522-9230-2025-19-142-147

Будник Людмила Андріївна,

кандидат економічних наук, доцент, доцент кафедри безпеки та правоохоронної діяльності Західноукраїнського національного університету

l.budnyk@wunu.edu.ua

ORCID ID: 0000-0002-1393-9354

Ронська Ольга Григорівна ,

кандидат економічних наук, доцент кафедри безпеки та правоохоронної діяльності Західноукраїнського національного університету

o.ronska@wunu.edu.ua

ORCID ID: 0000-0002-9856-3105

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У РОЗСЛІДУВАННІ ПРАВОПОРУШЕНЬ З КРИПТОАКТИВАМИ

Стаття присвячена аналізу міжнародного співробітництва у розслідуванні кримінальних правопорушень, пов'язаних із криптоактивами, актуальність якого зумовлена стрімким зростанням транскордонних цифрових злочинів та ускладненням ідентифікації правопорушників у децентралізованому середовищі блокчейну. Метою дослідження є визначення правових, інституційних і технологічних засад міжнародної взаємодії, а також окреслення проблем та перспектив удосконалення глобальних механізмів протидії криптозлочинності. У роботі застосовано аналіз нормативної бази, порівняльно-правовий метод, огляд міжнародних стандартів FATF, практики Європолу, Інтерполу та інших організацій, а також дослідження інструментів блокчейн-аналітики. Результати демонструють, що ефективність розслідувань залежить від стандартизації обміну інформацією, швидкого доступу до цифрових доказів, узгодження регуляторних підходів різних держав та активної взаємодії з приватними аналітичними компаніями. Визначено ключові проблеми: повільність процедур міжнародної правової допомоги, відмінності у правовому статусі криптоактивів, складність арешту й конфіскації цифрових активів, а також обмеженість державного впливу на децентралізовані системи. Автор підкреслює, що гармонізація законодавств, імплементація глобальних стандартів та розвиток спільних слідчих механізмів є фундаментом для підвищення ефективності боротьби з транснаціональною цифровою злочинністю.

Ключові слова: криптоактиви; міжнародне співробітництво; блокчейн-аналітика; розслідування злочинів; FATF; цифрова криміналістика; транскордонна злочинність; правова допомога.

Budnyk L., Ronska O. INTERNATIONAL COOPERATION IN THE INVESTIGATION OF OFFENSES INVOLVING CRYPTO ASSETS

The article examines the international cooperation mechanisms used in investigating criminal offenses involving crypto-assets, emphasizing their growing relevance amid the rapid global expansion of blockchain technologies and the increasing scale of cross-border digital crime. The study highlights that the decentralized architecture of most cryptocurrencies, the speed of transactions, and the potential for partial anonymity create significant challenges for national law-enforcement agencies and require coordinated international responses. The aim of the research is to comprehensively analyze the legal, institutional, and technological foundations of global cooperation in the field of crypto-asset investigations, identify existing gaps in intergovernmental interaction, and outline pathways to enhance the effectiveness of international crime-control mechanisms.

The methodology is based on comparative legal analysis, examination of regulatory standards, review of international practices (Europol, Interpol, FATF), and assessment of technological tools used in blockchain forensics. The study demonstrates that efficient investigations depend on harmonized regulatory frameworks, standardized information-exchange procedures, and timely access to digital evidence, which often disappears within hours due to the technical nature of blockchain networks. The results show the crucial role of FATF standards, the “travel rule,” joint investigation teams, digital forensic instruments, and public-private cooperation involving blockchain analytics companies such as Chainalysis or TRM Labs.

The article identifies major challenges: differences in national legal regimes regarding the status of crypto-assets, bureaucratic delays in mutual legal assistance procedures, limited state control over decentralized systems, and the complexity of freezing or confiscating crypto-assets across jurisdictions. It concludes that strengthening global cybersecurity and combating transnational crypto-related crime require a comprehensive model of cooperation that integrates legal, technological, organizational, and forensic components, as well as further harmonization of international standards in the digital-asset sphere.

Keywords: crypto assets; international cooperation; blockchain analytics; crime investigation; FATF standards; digital forensics; cross-border crime; legal assistance.

Постановка проблеми. Міжнародне співробітництво у розслідуванні злочинів, пов'язаних із криптоактивами, стає одним із ключових напрямів сучасної криміналістики, оскільки цифровізація фінансової сфери спричиняє появу нових форм злочинної діяльності, що виходять за межі традиційних юрисдикційних підходів. За попередніми оцінками, упродовж 2024 року на адреси, пов'язані з незаконною діяльністю – зокрема криптогаманці або інші криптовалютні реквізити, що використовуються у протиправних цілях – було переказано 40,9 млрд доларів США. З 2020 року втрати від діяльності криптозлочинців щороку зростали в середньому на 24% [1]. У глобалізованому просторі криптоактиви дають можливість здійснювати швидкі, транскордонні, частково анонімні трансакції, які ускладнюють ідентифікацію правопорушників та джерел походження коштів. Відповідно, ефективне реагування на такі виклики потребує скоординованих зусиль між державами, міжнародними організаціями, правоохоронними структурами та приватним сектором, зокрема постачальниками послуг у сфері віртуальних активів, аналітичними компаніями та фінансовими інституціями. Науковий аналіз цієї проблематики передбачає ґрунтовне дослідження міжнародно-правових механізмів співробітництва, інструментів обміну інформацією, особливостей слідчої діяльності у сфері криптоактивів, а також визначення напрямів удосконалення міждержавної взаємодії.

Аналіз останніх досліджень та публікацій. Дослідження у сфері міжнародної протидії злочинам, пов'язаним із криптоактивами, свідчать про стрімке зростання уваги держав, міжурядових організацій та дослідницьких центрів до проблеми транскордонної природи цих правопорушень. У науковій літературі підкреслюється, що децентралізований характер блокчейну, а також можливість здійснювати фінансові операції поза межами традиційної банківської системи створюють суттєві виклики для правоохоронних органів різних країн. Дослідники також виділяють тенденцію до збільшення кількості злочинів, які використовують криптоактиви для фінансування діяльності міжнародних злочинних угруповань, кіберзлочинності, ухилення від санкцій та відмивання коштів [2].

У публікаціях останніх років акцент робиться на ролі міжнародних механізмів координації, серед яких провідне місце займають Європол, Інтерпол, FATF та спільні слідчі групи (JITs). Європол у своїх аналітичних звітах наголошує на необхідності стандартизації обміну інформацією про криптовалютні трансакції та вдосконаленні інструментів ідентифікації власників цифрових гаманців. Інтерпол, зі свого боку, впроваджує глобальні ініціативи зі створення баз даних криптоадрес, пов'язаних зі злочинною діяльністю, а також розвиває співпрацю з приватними компаніями, що займаються блокчейн-аналітикою [3; 4].

Науковці відзначають, що одним із найбільш досліджуваних напрямів є робота FATF, яка розробляє міжнародні стандарти щодо боротьби з відмиванням коштів та фінансуванням тероризму за участі криптоактивів. У той же час автори наголошують на складнощях імплементації цих норм у країнах із різним рівнем технологічного розвитку та відмінними правовими режимами [5; 6].

Важливе місце в сучасній літературі займають питання взаємодії державних органів із приватними аналітичними компаніями (Chainalysis, TRM Labs, Elliptic). Дослідники підкреслюють, що саме приватний сектор створює інноваційні інструменти для візуалізації трансакцій, деанонізації учасників та відстеження руху цифрових активів. Натомість ефективність міжнародного співробітництва залежить від доступу правоохоронців до таких технологій, а також рівня підготовки фахівців [7, с.23].

Таким чином, сучасні дослідження демонструють, що міжнародне співробітництво у розслідуванні злочинів з криптоактивами перебуває на етапі активного розвитку, і ключовими факторами успіху є технологічне оновлення, уніфікація нормативних стандартів та поглиблення партнерства між державними та приватними структурами.

Мета статті полягає у всебічному аналізі правових та інституційних засад міжнародного співробітництва в розслідуванні кримінальних правопорушень із використанням криптоактивів, з'ясуванні наявних проблем у взаємодії між державами та визначення напрямів підвищення ефективності глобального механізму протидії таким правопорушенням.

Виклад основного матеріалу дослідження. У сучасних умовах розслідування злочинів із використанням криптоактивів характеризується транснаціональною природою, що зумовлено децентралізованим характером блокчейн-технологій. Для транснаціональної злочинності криптоактиви цікаві своїми властивостями (рис.1).

Більшість криптоактивів функціонує у розподілених мережах, які не мають фізичного центру або адміністративної юрисдикції. Унаслідок цього злочини, пов'язані з відмиванням коштів, кібершахрайством, незаконним обігом наркотиків, фінансуванням тероризму та іншими правопорушеннями, здійснюються через цифрові канали, що охоплюють різні континенти. Тому ключовою передумовою ефективного розслідування є налагодження швидкої комунікації між правоохоронними органами різних країн, а також розроблення уніфікованих стандартів реагування [8]. Слід враховувати, що багато важливих цифрових доказів може зникнути за лічені години, а тому затримки у міжнародних запитах про правову допомогу нерідко призводять до втрати цінної інформації.

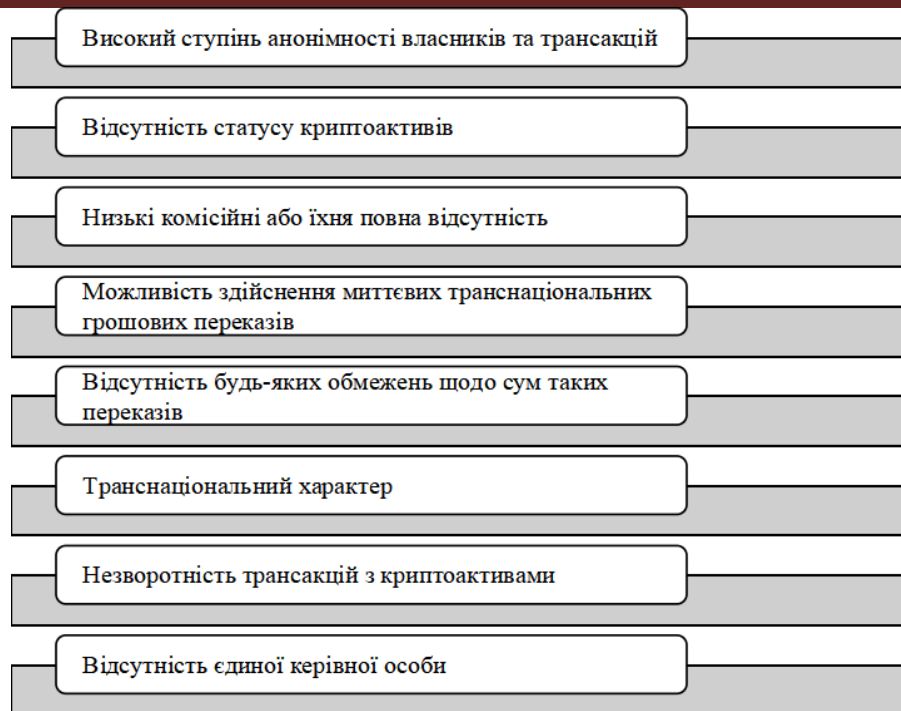


Рис.1. Властивості трансакцій з криптоактивами

Стандарти ФАТФ щодо регулювання постачальників послуг віртуальних активів суттєво впливають на формування національних законодавств, сприяючи гармонізації правових норм та запровадженню глобального підходу «travel rule», який передбачає передавання необхідної інформації про учасників криптотранзакцій [9]. Це дозволяє зменшити рівень анонімності та забезпечити можливість ідентифікації правопорушників у випадку незаконних операцій. У свою чергу, взаємодія правоохоронних органів у рамках Європолу та Інтерполу передбачає обмін оперативними даними, проведення спільних операцій, організацію тренінгів, а також розроблення спеціалізованих методичних рекомендацій щодо розслідування злочинів із криптоактивами.

Процес розслідування злочинів, пов'язаних із криптоактивами, передбачає тісну взаємодію правоохоронних органів із приватним сектором. Криптовалютні біржі, провайдери кастодіальних та некостодіальних гаманців, майнінгові пули, оператори платіжної інфраструктури та інші учасники криптоекономіки володіють великою кількістю технічних і персональних даних, які можуть мати доказове значення під час кримінального провадження. У більшості юрисдикцій законодавство покладає на такі компанії обов'язок здійснювати процедури KYC/AML (ідентифікацію та верифікацію клієнтів, моніторинг операцій), зберігати журнали трансакцій, IP-адрес та іншу інформацію, а також оперативно передавати відповідні дані правоохоронним органам у разі виявлення підозрілої чи незаконної активності. Наприклад, у Сполучених Штатах Америки фінансові установи, включно з криптовалютними біржами, підпадають під регулювання FinCEN. Вони зобов'язані проводити комплексні процедури KYC/AML, подавати Звіти про підозрілу активність (SARs), а також зберігати докладні журнали операцій. Окремі регулятори штатів (наприклад, Нью-Йоркський департамент фінансових послуг із вимогами BitLicense) вимагають від компаній ширшого масиву даних і підвищеного рівня комплаєнсу. Це створює багаторівневу систему контролю, яка забезпечує можливість оперативного отримання правоохоронцями інформації під час розслідувань.

У Європейському Союзі криптокомпанії регулюються регламентом MiCA, який встановлює єдині стандарти для провайдерів послуг із криптоактивами. Платформи повинні здійснювати ідентифікацію клієнтів, вести облік трансакцій, повідомляти про підозрілу діяльність та у деяких випадках виконувати вимоги щодо «подорожного правила» для переведення інформації про відправника й отримувача між різними сервісами [10]. ЄС прагне створити уніфіковану систему, що полегшує обмін даними між країнами-членами під час кримінальних проваджень.

Ефективність міжнародного співробітництва у сфері криптоактивів залежить від узгодження регуляторних підходів між різними державами. Гармонізація вимог щодо комплаєнсу, обміну інформацією та стандартів цифрової ідентифікації сприяє формуванню більш передбачуваного й уніфікованого глобального регуляторного середовища для боротьби зі злочинами, пов'язаними з криптоактивами. Важливою проблемою залишається гармонізація національних законодавств щодо криптоактивів. Різні країни застосовують різні підходи до правового статусу криптовалют, що створює бар'єри для ефективного міжнародного співробітництва. У деяких юрисдикціях криптоактиви розглядаються як майно, у інших - як фінансові інструменти або цифрові товари. Такі розбіжності ускладнюють процедури арешту та конфіскації

криптоактивів, а також впливають на порядок обміну інформацією між компетентними органами. Що стосується вітчизняного законодавства, то станом на осінь 2025 року Закон України «Про віртуальні активи» усе ще не набрав чинності через відсутність необхідних змін до податкового законодавства. Регулювання криптоактивів залишається неповним і базується переважно на загальних положеннях Цивільного, Податкового та Кримінального кодексів. При цьому у кримінальних провадженнях, що стосуються криптоактивів, правоохоронні органи здебільшого зосереджуються на доведенні фактичного володіння активами, а не на застосуванні спеціальних нормативних актів. Унаслідок цього адвокати, які працюють з такими справами, повинні спиратися на сформовану судову практику, технічну природу криптоактивів та особливості кожного конкретного виду доказів [11]. Уніфікація правових норм дозволила б забезпечити більш ефективну взаємодію під час розслідування злочинів із криптоактивами, а також створила б прозорі умови для функціонування міжнародного ринку цифрових активів.

Не менш важливою проблемою є конфіскація криптоактивів. Доцільно зазначити, що станом на сьогодні жодна держава у світі не має повноцінного, практично ефективного та універсально застосовного механізму, який би гарантував захист прав власника цифрових грошей на рівні, співставному з традиційними фінансовими інструментами. Навіть країни з розвиненим регулюванням криптоактивів, такі як США, Сінгапур, Швейцарія чи держави ЄС, не здатні забезпечити власникам криптовалют абсолютних юридичних гарантій або повного контролю над діяльністю всіх учасників криптовалютного середовища. Це обумовлено низкою факторів. Перш за все, технічна архітектура більшості криптовалют (зокрема, децентралізованих блокчейнів) не дозволяє державним органам втручатися в транзакції, скасовувати або повернути цифрові перекази, блокувати активи на рівні протоколу чи забезпечувати ідентифікацію сторін без участі приватних сервісів. У разі втрати приватного ключа, хакерських атак або шахрайства юридичні механізми відшкодування є обмеженими: держава не може примусово «повернути» криптоактиви так само, як у випадку з банківськими рахунками чи звичайними фінансовими операціями.

Крім того, більшість суб'єктів криптоекосистеми, від глобальних бірж до DeFi-платформ, часто працюють у транскордонному режимі, використовуючи різні юрисдикції або розподілені мережі без централізованого оператора. Навіть США та ЄС, які мають потужні регуляторні інструменти (FinCEN, SEC, CFTC, MiCA, AMLD тощо), не володіють засобами примусового впливу на децентралізовані протоколи, операторів, що працюють анонімно, або компанії, які фізично не розміщені в межах їхньої територіальної компетенції.

У підсумку відсутність єдиного міжнародного підходу, децентралізована природа технології та різноманіття правових режимів призводять до того, що жодна держава не може гарантувати ані абсолютного захисту прав власника цифрових грошей, ані безумовного регуляторного впливу на всіх учасників криптовалютних відносин. Це створює правовий вакуум і водночас підкреслює необхідність подальшої гармонізації міжнародних стандартів та розвитку глобальних механізмів координації у сфері цифрових активів. Навіть якщо правоохоронні органи ідентифікували правопорушника та цифрові активи, що належать йому, процес вилучення таких активів може бути складним з огляду на технологічну специфіку блокчейну та необхідність отримання міжнародної правової допомоги. Спільні підходи до реалізації таких активів, їхнього перерахування до бюджету або передачі потерпілим є важливою передумовою для підвищення ефективності боротьби з транснаціональною злочинністю.

Висновки. Міжнародне співробітництво у розслідуванні злочинів, пов'язаних із криптоактивами, є критично важливим елементом глобальної протидії цифровій злочинності, що набуває дедалі більшого масштабу в умовах стрімкої еволюції блокчейн-технологій. Децентралізований характер криптовалют, швидкість транзакцій та можливість часткової анонімності створюють суттєві перешкоди для національних правоохоронних органів, тому лише узгоджені міждержавні дії можуть забезпечити ефективне розслідування таких правопорушень.

Гармонізація законодавств, імплементація стандартів ФАТФ, удосконалення механізмів міжнародної правової допомоги, розвиток пришвидшених процедур обміну інформацією та створення спільних слідчих груп формують основу для підвищення результативності боротьби з кримінальними діями у сфері криптоактивів. Значну роль у цьому відіграють міжнародні організації, а також приватні компанії, що спеціалізуються на блокчейн-аналітиці й володіють важливими технологічними ресурсами.

Особливе значення має цифрова криміналістика, оскільки можливість відстеження руху криптовалют та ідентифікації учасників транзакцій стає провідним інструментом для збору доказів у транснаціональних справах.

Отже, міжнародна взаємодія у розслідуванні злочинів із криптоактивами має ґрунтуватися на комплексному підході, що поєднує правові, технологічні, криміналістичні та організаційні аспекти. Лише така модель здатна забезпечити ефективне реагування на нові форми транснаціональної цифрової злочинності та сприяти зміцненню глобальної кібербезпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. The Chainalysis 2025 Crypto Crime Report URL: <https://go.chainalysis.com/2025-Crypto-Crime-Report.html> (дата звернення: 10.09.2025)

2. Старушенко Я.В. Зарубіжний досвід правового регулювання запобігання відмиванню коштів отриманих від обігу віртуальних активів. *Юридичний науковий електронний журнал*. № 7/2025. С.302-304. DOI <https://doi.org/10.32782/2524-0374/2025-7/67>
3. Яцик Т.П., Шкелебей В.А. Міжнародна співпраця під час розслідування кримінальних правопорушень, пов'язаних з обігом віртуальних активів. *Освіта і наука*. 2023. Випуск 2(35). С. 343-351. URL: <https://ekmair.ukma.edu.ua/server/api/core/bitstreams/654e82b9-f0bf-4a2a-9c81-148feeaa6901/content> (дата звернення: 10.09.2025)
4. Кузьменко О. В., Карпюк І. С. Розслідування легалізації (відмивання) доходів, отриманих злочинним шляхом із використанням віртуальних валют: методичні рекомендації. URL: http://www.lsej.org.ua/8_2020/107.pdf.
5. Бохенко В.М. Кримінологічні ризики обігу криптовалюти. URL: <https://doi.org/10.32782/2524-0374/2021-12/82> (дата звернення: 12.09.2025)
6. Доляновська І.М., Кривенко К.О. Світовий досвід протидії кримінальним правопорушенням, пов'язаним з обігом віртуальних активів. *Legal Bulletin*. 2024. №12. С. 79–86. <https://doi.org/10.31732/2708-339X-2024-12-A12>
7. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. Київ, 2024. №1. 327 с.
8. Movchan, A., Shliakhovskiy, O., Kozii, V., & Fedchak, I. Investigating cryptocurrency financing crimes terrorism and armed aggression. *Social and Legal Studios*, 2023. №6(4), С.123-131 <https://doi.org/10.32518/sals4.2023.123>.
9. FATF (2023). Цільове Оновлення в Контексті Імплементції Стандартів FATF щодо Віртуальних Активів та Постачальників Послуг з Віртуальними Активами. Париж. URL: <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html> (дата звернення: 13.09.2025)
10. Будник Л.А., Будник В.І. Правове регулювання ринку цифрових активів. *Матеріали III Міжнародної науково-практичної конференції «Сучасне управління організаціями: концепції, цифрові трансформації, моделі інноваційного розвитку»*. Харків. 2023 р. С.56-59 URL: <https://ekhnur.karazin.ua/server/api/core/bitstreams/6c453407-c526-4016-80c1-beb2e5b79fae/content> (дата звернення: 14.09.2025)
11. Лукінчук Р., Пенкіна А. Доведення факту володіння криптовалютою у кримінальному процесі: джерела та інструменти. URL: <https://advanq.ua/dovedennya-faktu-volodinnya-kriptovalyutoyu-u-kriminalnomu-proczesi-dzherela-ta-instrumenti/> (дата звернення: 11.09.2025)

REFERENCES:

1. Chainalysis. (2025). The Chainalysis 2025 Crypto Crime Report. Retrieved from <https://go.chainalysis.com/2025-Crypto-Crime-Report.html> [in English].
2. Starushchenko, Ya. V. (2025). Zarubizhnyi dosvid pravovoho rehuliuвання zapobihannya vidmyvanniu koshtiv otrymanykh vid obihu virtualnykh aktyviv [Foreign experience of legal regulation of preventing money laundering derived from virtual asset circulation]. *Yurydychnyi naukovyi elektronnyi zhurnal*, 7, 302–304. <https://doi.org/10.32782/2524-0374/2025-7/67> [in Ukrainian].
3. Yatsyk, T. P., & Shkelebei, V. A. (2023). Mizhnarodna spivpratsia pid chas rozsliduvannya kryminalnykh pravoporushen, pov'iazanykh z obihom virtualnykh aktyviv [International cooperation in the investigation of criminal offenses related to virtual asset circulation]. *Osvita i Nauka*, 2(35), 343–351. Retrieved from <https://ekmair.ukma.edu.ua/server/api/core/bitstreams/654e82b9-f0bf-4a2a-9c81-148feeaa6901/content> [in Ukrainian].
4. Kuzmenko, O. V., & Karpiuk, I. S. (2020). Rozsliduvannya lehalizatsii (vidmyvannia) dokhodiv, otrymanykh zlochnym shliakom iz vykorystanniam virtualnykh valiut: metodychni rekomendatsii [Investigation of legalization (laundering) of criminal proceeds using virtual currencies: methodological recommendations]. Retrieved from http://www.lsej.org.ua/8_2020/107.pdf [in Ukrainian].
5. Bokhenko, V. M. (2021). Kryminolohichni ryzyky obihu kryptovaliut [Criminological risks of cryptocurrency circulation]. <https://doi.org/10.32782/2524-0374/2021-12/82> [in Ukrainian].
6. Dolianovska, I. M., & Kryvenko, K. O. (2024). Svitovyi dosvid protydyi kryminalnym pravoporushenniam, pov'iazanykh z obihom virtualnykh aktyviv [Global experience in combating criminal offenses related to virtual asset circulation]. *Legal Bulletin*, 12, 79–86. <https://doi.org/10.31732/2708-339X-2024-12-A12> [in Ukrainian].
7. Dovhan, O., Lytvynova, L., & Dorohykh, S. (Eds.). (2024). Kiberbezpeka v informatsiinomu suspilstvi: informatsiino-analitychnyi daidzhest [Cybersecurity in the information society: informational-analytical digest]. Kyiv: Instytut informatsii, bezpeky i prava NAPrN Ukrainy; Vernadskyi National Library of Ukraine. No. 1, 327 p. [in Ukrainian].

8. Movchan, A., Shliakhovskiy, O., Kozii, V., & Fedchak, I. (2023). Investigating cryptocurrency financing crimes terrorism and armed aggression. *Social and Legal Studios*, 6(4), 123–131. <https://doi.org/10.32518/sals4.2023.123> [in English].

9. FATF. (2023). *Tsilove Onovlennia v Konteksti Implementatsii Standartiv FATF shchodo Virtualnykh Aktyviv ta Postachal'nykiv Posluh z Virtual'nymy Aktyvamy* [Targeted update on the implementation of FATF standards on virtual assets and virtual asset service providers]. FATF, Paris. Retrieved from <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html> [in Ukrainian].

10. Budnyk, L. A., & Budnyk, V. I. (2023). *Pravove rehuliuвання rynku tsyfrovyykh aktyviv* [Legal regulation of the digital asset market]. In *Proceedings of the III International Scientific and Practical Conference "Suchasne upravlinnia orhanizatsiiamy: kontseptsii, tsyfrovi transformatsii, modeli innovatsiinoho rozvytku"* (pp. 56–59). Kharkiv. Retrieved from <https://ekhnur.karazin.ua/server/api/core/bitstreams/6c453407-c526-4016-80c1-beb2e5b79fae/content> [in Ukrainian].

11. Lukinchuk, R., & Penkina, A. (n.d.). *Dovedennia faktu volodinnia kryptovaliutoiu u kryminalnomu protsesi: dzherela ta instrumenty* [Proving cryptocurrency ownership in criminal proceedings: sources and tools]. Retrieved from <https://advanq.ua/dovedennya-faktu-volodinnya-kriptovalyutoyu-u-kryminalnomu-proczeni-dzherela-ta-instrumenti/> [in Ukrainian].

Стаття надійшла до редакції: 10.11.2025

УДК 343.13:004

DOI: 10.36550/2522-9230-2025-19-147-151

Мехеда Владислав Дмитрович,

кандидат юридичних наук,

заступник начальника кафедри соціально-гуманітарних дисциплін

Військового інституту танкових військ

Національного технічного університету «Харківський політехнічний інститут»

mekhedavd@ukr.net

ORCID ID: 0000-0002-2160-3738

ДОКАЗУВАННЯ У КРИМІНАЛЬНОМУ ПРОЦЕСІ В УМОВАХ ЦИФРОВІЗАЦІЇ: ЄВРОПЕЙСЬКІ СТАНДАРТИ ТА УКРАЇНСЬКІ РЕАЛІЇ

У статті досліджено сучасний стан доказування у кримінальному процесі України в умовах цифрової трансформації суспільства. Підкреслюється, що доказування є фундаментальною складовою реалізації принципів верховенства права, презумпції невинуватості та справедливого суду. З появою нових технологій традиційна система доказів доповнюється електронними даними, цифровими документами, записами з мережі Інтернет та іншими інформаційними джерелами, що суттєво змінює підходи до оцінки доказів.

Актуальність теми зумовлена необхідністю гармонізації національного кримінального процесуального законодавства з європейськими стандартами та міжнародними практиками у сфері збирання, збереження й перевірки електронних доказів. Відсутність чітких критеріїв автентичності, процедур «ланцюга збереження» (chain of custody) та механізмів верифікації цифрових даних створює ризики для дотримання прав людини та справедливості судового розгляду.

У роботі проаналізовано положення чинного Кримінального процесуального кодексу України, міжнародні акти Європейського Союзу, а також практику Європейського суду з прав людини щодо допустимості доказів. Наголошено, що ключовим критерієм залишається не формальна відповідність доказу процесуальним вимогам, а забезпечення «справедливості в цілому».

Визначено перспективні напрями вдосконалення доказового процесу: нормативне закріплення поняття «електронний доказ» і процедур його перевірки, розроблення методичних рекомендацій щодо роботи з цифровими слідами, розвиток підготовки фахівців у сфері цифрової криміналістики та OSINT.

Додатково підкреслено, що успішне впровадження таких реформ потребує комплексного підходу, який включає не лише зміни законодавства та методичні рекомендації, а й розвиток сучасної матеріально-технічної бази, створення спеціалізованих лабораторій цифрової криміналістики та міжвідомчу координацію правоохоронних органів, судів і наукових установ. Такий підхід дозволить забезпечити ефективність доказового процесу в умовах цифрової трансформації, гарантувати дотримання прав людини та сприятиме формуванню високого рівня професійної компетентності фахівців у сфері сучасного кримінального провадження.

Зроблено висновок, що інтеграція європейських стандартів та запровадження єдиних правил поведінки з електронними доказами підвищить ефективність досудового розслідування, забезпечить прозорість судового процесу й зміцнить довіру суспільства до правосуддя.

Ключові слова: доказування, кримінальний процес, електронні докази, цифрові технології, допустимість