УДК 343.9:004.62+006.3/.8
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364550

Олександр Дмитрович Довгань
Державна наукова установа "Інститут інформації, безпеки і права Національної академії правових наук України".
Київ, Україна
ORCID: https://orcid.org/0000-0002-3453-4938
Тарас Юрійович Ткачук
Український науково-дослідний інститут спеціальної техніки та судових експертиз СБУ.
Київ, Україна
ORCID: https://orcid.org/0000-0002-4620-3300
Віталій Геннадійович Оніщенко
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Київ, Україна
ORCID: https://orcid.org/0009-0002-8165-0330

ЦИФРОВІ ЕКОНОМІЧНІ ДОКАЗИ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРАВОВІ ТА ЕКСПЕРТНІ ПІДХОДИ КРІЗЬ ПРИЗМУ СТАНДАРТІВ ЄС

Анотація. *Статтю присвячено дослідженню цифрових економічних доказів у кримінальному провадженні в умовах цифровізації фінансової злочинності, поширення криптоактивів і зростання значення блокчейн-записів, on-chain та off-chain даних, log-файлів і результатів алгоритмічного аналізу. Обґрунтовано, що розвиток нових форм економічної злочинності, зокрема пов'язаних з обходом санкцій, фінансуванням терористичної діяльності та використанням децентралізованих фінансових платформ, актуалізує потребу в належному правовому та експертному осмисленні цифрових економічних доказів.*

Основну увагу зосереджено на з'ясуванні правової природи цифрових економічних доказів, особливостей їх ідентифікації, аналізу, верифікації та процесуальної інтерпретації у кримінальному провадженні. Доведено, що ефективне дослідження таких доказів вимагає міждисциплінарного підходу, який поєднує економічний аналіз, цифрову криміналістику, блокчейн-аналітику, фінансовий моніторинг та інструменти штучного інтелекту і машинного навчання.

З урахуванням актуальних викликів, пов'язаних із використанням криптоактивів для обходу санкцій, фінансування терористичної діяльності та інших форм економічної злочинності, обґрунтовано необхідність переосмислення методологічних і організаційних засад експертної діяльності. Основну увагу зосереджено на аналізі регуляторного досвіду Європейського Союзу, зокрема в межах реалізації стратегічних рамок AMLA, DORA та MiCA.

Сформульовано висновки щодо доцільності імплементації в українську практику окремих положень європейських підходів, що сприятимуть підвищенню достовірності, професійності та міжнародного визнання судово-економічної експертизи у справах з цифровим компонентом.

Ключові слова: *цифрові економічні докази, кримінальне провадження, цифрові докази, судова експертиза, блокчейн-аналітика, криптоактиви, штучний інтелект, AMLA, DORA, MiCA, ЄС.*

Oleksandr D. Dovhan
State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-3453-4938
Taras Yu. Tkachuk
Ukrainian Research Institute of Special Equipment and Forensic Expertise of Security Service of Ukraine
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-4620-3300
Vitalii G. Onishchenko
Ukrainian Research Institute of Special Equipment and Forensic Expertise of Security Service of Ukraine
Kyiv, Ukraine
ORCID: https://orcid.org/0009-0002-8165-0330

DIGITAL ECONOMIC EVIDENCE IN CRIMINAL PROCEEDINGS: LEGAL AND EXPERT APPROACHES THROUGH THE PRISM OF EU STANDARDS

Summary. *The article is devoted to the study of digital economic evidence in criminal proceedings in the context of the digitalisation of financial crime, the spread of crypto-assets, and the growing importance of blockchain records, on-chain and off-chain data, log files, and the results of algorithmic analysis. It is substantiated that the development of new forms of economic crime, in particular those related to sanctions evasion, the financing of terrorist activities, and the use of decentralised financial platforms, intensifies the need for a proper legal and expert understanding of digital economic evidence.*

The main focus is placed on clarifying the legal nature of digital economic evidence, as well as the specific features of its identification, analysis, verification, and procedural interpretation in criminal proceedings. It is proved that the effective examination of such evidence requires an interdisciplinary approach combining economic analysis, digital forensics, blockchain analytics, financial monitoring, and artificial intelligence and machine learning tools.

Given the current challenges associated with the use of crypto-assets for sanctions evasion, the financing of terrorist activities, and other forms of economic crime, the need to rethink the methodological and organisational foundations of expert activity is substantiated. Particular attention is paid to the analysis of the regulatory experience of the European Union, especially within the framework of AMLA, DORA, and MiCA.

Conclusions are also drawn as to the expediency of implementing certain provisions of European approaches into Ukrainian practice, which would contribute to enhancing the reliability, professionalism, and international recognition of forensic economic examination in cases involving a digital component.

Keywords: *digital economic evidence, criminal proceedings, digital evidence, forensic examination, blockchain analytics, crypto-assets, artificial intelligence, AMLA, DORA, MiCA, EU.*

Постановка проблеми. Цифровізація фінансових відносин і стрімке поширення криптоактивів, децентралізованих фінансових платформ, блокчейн-технологій та алгоритмічних систем обробки даних істотно змінили не лише механізми вчинення фінансових злочинів, а й саму природу доказової інформації у кримінальному провадженні. Впродовж останніх років відбулися фундаментальні зміни природи фінансових злочинів. Обсяги незаконних транзакцій з використанням криптоактивів досягли рекордних показників (154 млрд доларів США у 2025 році), що на 162% більше

порівняно з попереднім роком [1]. Це свідчить про те, що використання віртуальних активів у злочинних цілях перетворилося на системну загрозу для міжнародної фінансової стабільності та національної безпеки держав. У сучасних умовах дедалі більшого значення набувають цифрові економічні докази, до яких належать блокчейн-записи, on-chain та off-chain дані, log-файли, цифрові сліди транзакцій, результати автоматизованого аналізу та інші інформаційні масиви, здатні підтверджувати фактичні обставини у справах про фінансові правопорушення.

Ключовим аспектом цієї загрози є не стільки кількісне зростання, скільки якісна зміна її характеру. Криптоактиви еволюціонували від інструменту для окремих злочинців до стратегічного вектора у веденні сучасних війн. Згідно з висновками звіту Europol EU-SOCTA 2025 [2] геополітичні супротивники все частіше використовують злочинних посередників для проведення руйнівних операцій проти урядів та критичної інфраструктури. Це призводить до виникнення "гібридних загроз", спрямованих на дестабілізацію суспільств, економік та демократичних інститутів. Для України, яка перебуває в стані війни, ця загроза є прямою та екзистенційною, адже віртуальні активи активно використовуються для фінансування терористичних і диверсійних груп, а також для систематичного обходу міжнародних санкцій, запроваджених проти держави-агресора.

Загроза посилюється стрімкою професіоналізацією злочинної діяльності у цифровому просторі. Зловмисники застосовують дедалі складніші тактики, техніки та процедури, що виходять далеко за межі аналітичних можливостей традиційного фінансового аудиту. Йдеться про використання децентралізованих бірж, міжланцюгових мостів, анонімних монет (наприклад, Monero) та складних сервісів для змішування транзакцій [3]. Усі ці інструменти розроблені з єдиною метою розірвати ланцюг доказів і зробити відстеження фінансових потоків практично неможливим для непідготовленого фахівця.

Додаткової актуальності темі надає те, що в українському кримінальному процесі та законодавстві про судову експертизу досі відсутні уніфіковані підходи до визначення, дослідження та процесуального використання цифрових економічних доказів. Водночас у праві Європейського Союзу вже формуються комплексні стандарти, які прямо або опосередковано впливають на цю сферу. Насамперед ідеться про AMLA як основу уніфікації підходів у сфері протидії відмиванню коштів і фінансуванню тероризму, DORA як нормативну модель оцінки цілісності та стійкості цифрової інфраструктури, а також MiCA як регуляторну основу класифікації криптоактивів і діяльності постачальників послуг, пов'язаних із ними. У сукупності ці стандарти формують нову нормативну й методичну рамку для осмислення цифрових економічних доказів у кримінальному провадженні.

Отже, актуальність обраної теми зумовлена потребою у формуванні сучасного правового та експертного підходу до цифрових економічних доказів, який би враховував технологічну природу нових джерел інформації, процесуальні вимоги кримінального провадження та перспективи гармонізації української практики зі стандартами Європейського Союзу.

Результати аналізу наукових публікацій. Теоретичну базу дослідження формують праці провідних вітчизняних і зарубіжних науковців. Значну увагу питанням змісту та меж спеціальних знань судового експерта присвячено у працях В. Шепітька, В. Гончаренка, М. Щербаковського, а також у дослідженнях О. Горлачука, які окреслюють методологічні основи судово-економічної експертизи. Актуальні виклики, пов'язані з адаптацією криміналістики до цифрових реалій, висвітлюються у роботах О.

Шевчука, П. Ріді, Н. Гартт, Дж. Халілі та інших дослідників, що досліджують межі допустимості цифрових доказів, інституціоналізацію блокчейн-аналітики та розвиток цифрової криміналістики в контексті кримінального правосуддя.

Водночас аналіз наявної літератури свідчить, що попри значну увагу до окремих аспектів цифрової криміналістики, криптоактивів і судової експертизи, у вітчизняній науці поки що відсутнє цілісне дослідження, у якому цифрові економічні докази були б розглянуті як самостійний предмет правового та експертного осмислення у кримінальному провадженні. Недостатньо розробленими залишаються питання їх понятійного визначення, класифікації, процесуального статусу, критеріїв допустимості, відтворюваності та верифікації, а також ролі судового експерта у перетворенні розрізнених цифрових слідів на цілісну доказову інформацію.

Саме ця наукова прогалина зумовлює потребу у подальшому дослідженні цифрових економічних доказів крізь призму поєднання правових, криміналістичних, економічних і технологічних підходів, а також з урахуванням стандартів Європейського Союзу як орієнтира для розвитку національної правозастосовної та експертної практики.

Метою статті є дослідження правової природи цифрових економічних доказів у кримінальному провадженні, з'ясування особливостей їх експертного дослідження та визначення можливостей імплементації стандартів ЄС у національну практику роботи з такими доказами.

Виклад основного матеріалу. У сучасному кримінальному провадженні у справах про фінансові злочини дедалі більшого значення набувають цифрові економічні докази як особливий різновид доказової інформації, що формується у цифровому фінансовому середовищі. Йдеться про блокчейн-записи, on-chain та off-chain дані, log-файли, дані криптовалютних транзакцій, результати алгоритмічного аналізу, відомості KYC/AML, а також інші цифрові сліди, здатні підтверджувати обставини, пов'язані з рухом активів, економічним змістом операцій, джерелом коштів, характером фінансових зв'язків та ознаками протиправної діяльності. На початку 2026 року Європейський Союз переживає найбільш масштабні зміни у сфері протидії фінансовим злочинам за останні десятиліття [4]. Цифровізація фінансових операцій, запровадження єдиних регуляторних стандартів та стрімкий розвиток технологій штучного інтелекту докорінно змінюють підходи до виявлення та розслідування фінансових злочинів. Ці процеси безпосередньо впливають на вимоги до експертної діяльності у сфері економічних розслідувань. Важливим каталізатором цих змін стало започаткування повноцінної діяльності Європейського органу з питань боротьби з відмиванням коштів (AMLA) [5], стратегічні документи якого (SPD 2026-2028) [6] передбачають створення зводу правил з протидії відмиванню коштів та фінансуванню тероризму (AML/CFT Rulebook), формування централізованої цифрової екосистеми даних та впровадження аналітики на основі штучного інтелекту та машинного навчання (AI/ML-аналітика) у процеси фінансового нагляду.

Правова специфіка цифрових економічних доказів полягає в тому, що вони виникають на перетині кількох сфер: кримінального процесу, фінансового моніторингу, цифрової криміналістики, обігу криптоактивів і технологій аналітичної обробки даних. На відміну від традиційних документів централізованого обліку, такі дані часто мають фрагментарний, технічний, псевдонімний або алгоритмічно сформований характер. У зв'язку з цим їх доказове значення не є самоочевидним і потребує спеціальної процедури виявлення, верифікації, автентифікації та процесуальної інтерпретації. Саме тому ключового значення набуває питання не лише про наявність цифрового сліду, а

про можливість його перетворення на належний, допустимий, достовірний і відтворюваний доказ у кримінальному провадженні.

Як бачимо, розвиток науково-технічного прогресу суттєво розширив інструментарій судово-експертної діяльності, сприяючи формуванню категорії "спеціальні знання" як фундаментального поняття судової експертизи. Постійне вдосконалення фінансових технологій, поява нових форм економічної злочинності та складність схем ухилення від фінансового контролю вимагають адаптації методологічного апарату судової експертизи до сучасних реалій.

Аналіз доктринальних підходів до визначення спеціальних знань показує їхню орієнтацію переважно на формальну освіту, професійну спеціалізацію та галузеву специфіку знань у галузях науки, техніки чи ремесла. Так, В. Шепітько характеризує їх як сукупність сучасних знань в окремих галузях науки, техніки, мистецтва чи ремесла, підкреслюючи галузеву специфіку [7, с. 207]. В. Гончаренко акцентує на професійній спеціалізації, що застосовується для отримання доказової інформації спеціально підготовленими особами [8, с. 5]. О. Горлачук визначає їх як відомості, що не є загальновідомими та володіє ними обмежене коло осіб [9]. М. Щербаковський пропонує комплексне визначення, характеризуючи спеціальні знання як професійні компетенції, сформовані в результаті формальної освіти та практичного досвіду, що реалізуються через використання науково-технічних засобів при проведенні експертних досліджень [10, с. 3].

Аналіз доктринальних підходів до визначення спеціальних знань свідчить, що вони традиційно пов'язуються з формальною освітою, професійною спеціалізацією та галузевою належністю знань у сфері науки, техніки, мистецтва чи ремесла. Такий підхід має фундаментальне значення для теорії судової експертизи, однак він формувався переважно щодо об'єктів, які існують у межах централізованих систем обліку та класичних документальних джерел інформації. Натомість у сучасних кримінальних провадженнях про фінансові злочини дедалі частіше предметом дослідження стають цифрові економічні докази, що виникають у децентралізованому, псевдонімному та алгоритмічно керованому фінансовому середовищі.

За таких умов змінюється не лише технічний інструментарій експерта, а й сам характер спеціальних знань, необхідних для належної правової та економічної інтерпретації цифрових слідів. Якщо у традиційній моделі об'єктом аналізу були банківські виписки, бухгалтерські документи чи інші носії централізованого обліку, то нині йдеться про блокчейн-записи, дані криптовалютних транзакцій, log-файли, результати алгоритмічного аналізу, відомості KYC/AML та інші цифрові масиви, доказове значення яких не є самоочевидним і потребує спеціальної верифікації, автентифікації та процесуального осмислення.

Саме це зумовлює виникнення доктринального вакууму, що проявляється насамперед у відсутності єдиного понятійного апарату для позначення компетентності, необхідної для дослідження цифрових економічних доказів. Поняття "судово-економічна експертиза" та "комп'ютерно-технічна експертиза" окремо не охоплюють повною мірою того міждисциплінарного синтезу, який є необхідним для роботи з доказами у справах про фінансові злочини з цифровим компонентом. У першому випадку недостатньо враховується технічна природа цифрового сліду, у другому його економічний зміст і фінансово-правовий контекст.

З огляду на це доцільно запропонувати для наукової дискусії категорію "*спеціальні кіберекономічні знання"* (СКЕЗ), під якою слід розуміти інтегровану сукупність професійних компетенцій, методів і процедур, що поєднують економічний аналіз,

цифрову криміналістику, блокчейн-аналітику, роботу з даними та інструменти алгоритмічної верифікації з метою ідентифікації, аналізу, перевірки та інтерпретації цифрових економічних доказів у кримінальному провадженні. У такому розумінні йдеться не про механічне поєднання двох традиційних спеціальностей, а про формування міждисциплінарної моделі професійної компетентності, релевантної новому типу доказової інформації.

Структурно спеціальні кіберекономічні знання охоплюють щонайменше кілька взаємопов'язаних блоків: по-перше, економіко-фінансовий аналіз, спрямований на встановлення реального змісту транзакцій, руху активів, джерел коштів і ризиків, пов'язаних із відмиванням коштів, обходом санкцій чи фінансуванням терористичної діяльності; по-друге, криміналістично-технічні процедури, пов'язані з виявленням, збереженням, перевіркою цілісності та відтворюваності цифрових слідів; по-третє, аналітику даних і алгоритмічну верифікацію, що охоплює кластеризацію адрес, виявлення аномалій, документування параметрів моделей та перевірку відтворюваності отриманих результатів; по-четверте, процесуальні механізми, пов'язані з допустимістю цифрових доказів, доступом до off-chain джерел та належним документуванням результатів дослідження.

У межах запропонованого підходу *цифрову судово-економічну експертизу* (ЦСЕ) доцільно розглядати не стільки як вже сформовану нормативну спеціальність, скільки як перспективну процесуально-експертну модель дослідження цифрових економічних доказів. Її сутність полягає у реалізації спеціальних кіберекономічних знань для встановлення фактичного економічного змісту цифрових слідів, їх співвіднесення з on-chain та off-chain даними та формування науково обґрунтованого висновку, релевантного для кримінального провадження.

У цьому сенсі цифрова судово-економічна експертиза постає як форма процесуального перетворення фрагментарних технічних даних на цілісну доказову інформацію. Її завданням є не лише опис цифрових артефактів, а й перевірка їхньої достовірності, відтворюваності, економічної значущості та юридичної релевантності. Саме тому ключовою особливістю такої експертної діяльності є здатність поєднати технічний аналіз цифрового сліду з його економічною інтерпретацією у спосіб, що відповідає вимогам кримінального процесу.

Сучасний розвиток цифрової криміналістики й цифрових доказів [11-13] дає підстави для наукової дискусії щодо доцільності виокремлення "цифрової судово-економічної експертизи" як перспективного напряму розвитку судової експертизи в умовах цифровізації фінансових злочинів. У цьому контексті *цифрова судово-економічна експертиза* є процесуальною формою реалізації СКЕЗ, спрямованих на ідентифікацію, аналіз та інтерпретацію цифрових економічних доказів. Вона фокусується на дослідженні цифрових економічних доказів, зокрема блокчейн-даних, log-файлів, результатів аналізу Big Data і, на нашу думку, має розвиватися як перспективний міждисциплінарний напрям експертного дослідження цифрових економічних доказів, що інтегрує методи економічного аналізу та комп'ютерно-технічного дослідження в межах єдиної експертної спеціальності. Усе це свідчить насамперед про зростання потреби у міждисциплінарних дослідженнях у сфері фінансових злочинів. Існуючий інститут комплексної експертизи, безумовно, є важливим інструментом задоволення цієї потреби, і класичні експертні спеціальності зберігають свою актуальність. Водночас цифровізація фінансових злочинів створює запит на фахівця, який органічно поєднує економічні та цифрові компетенції в межах

єдиної спеціальності, що й обумовлює доцільність наукової дискусії щодо формування цифрової судово-економічної експертизи.

Ефективність ЦСЕ критично залежить від здатності експерта працювати з двома фундаментальними категоріями даних у криптоактивах: On-Chain та Off-Chain [13]. *On-Chain* (на-ланцюговий слід/дані) включає інформацію, яка незмінно та публічно записана безпосередньо у розподіленому реєстрі (блокчейні). Вона включає хеші транзакцій, адреси гаманців (псевдоніми), час, тип токену (наприклад, USDT, USDC або DAI – найпоширеніші стейблкоїни, що активно використовуються для обходу санкцій) та взаємодію зі смарт-контрактами. Ці дані є технічними артефактами злочину. Off-Chain інформація охоплює записи KYC/AML від криптобірж, банківські перекази, корпоративні документи та дані з відкритих джерел (OSINT). Для проведення експертизи слідчий надає експерту конкретні об'єкти дослідження, відповідні документи та їх копії, отримані в процесуальному порядку.

Показовим прикладом є справа United States v. Sterlingov (2024), розглянута в Окружному суді округу Колумбія, США. Романа Стерлінгова визнали винним у відмиванні коштів та незаконній діяльності з передачі коштів через криптомікшер Bitcoin Fog, через який пройшло понад 1,2 млн біткоїнів вартістю близько 400 млн доларів. Доказова база включала блокчейн-аналіз за допомогою програмного забезпечення Chainalysis Reactor, IP-аналіз, матеріали з онлайн-форумів та речові докази. Суд у рамках стандарту Daubert підтвердив наукову надійність методології блокчейн-аналізу та допустив відповідні експертні показання як докази [14]. Варто зазначити, що в американській системі статус "свідка-експерта" (expert witness) визначається не офіційною акредитацією, а науковою обґрунтованістю застосованої методології, що принципово відрізняється від української моделі залучення судового експерта.

При цьому справа наразі перебуває на стадії апеляційного оскарження, захист оскаржує наукову обґрунтованість методів блокчейн-криміналістики, зокрема достовірність атрибуції адрес та відсутність незалежної верифікації результатів до завершення судового розгляду. Це є досить важливим свідченням того, що на сьогодні у світовій практиці відсутні усталені, науково верифіковані та перевірені судовою практикою методики проведення експертних досліджень цифрових економічних доказів. Зазначена прогалина створює реальні ризики для доказової цінності експертних висновків і водночас визначає напрям подальших наукових досліджень щодо розробки стандартизованих, відтворюваних та процесуально допустимих методик цифрової судово-економічної експертизи, які б витримували перевірку як з боку захисту, так і з боку суду.

Ключова функція експерта, що володіє спеціальними кіберекономіними знаннями, полягає у науковому аналізі та злитті on-chain та off-chain даних. Ця діяльність відбувається у чітких процесуальних межах: експерт досліджує виключно ті об'єкти та матеріали, які були зібрані та надані йому органом досудового розслідування, і не виходить за межі поставлених питань.

У рамках такого дослідження він може застосовувати спеціалізовані методи для: аналізу on-chain артефактів, зокрема трасування фінансових потоків та виявлення зв'язків між цифровими гаманцями; кореляції on-chain результатів із наданими off-chain даними (наприклад, KYC-записами, банківськими документами) для формування обґрунтованого висновку; встановлення фактичного економічного змісту операцій, що слугує основою для подальшої правової оцінки, яку здійснюють слідчий та суд.

Таким чином, можна припустити, що саме здатність експерта до наукового злиття цих типів даних є одним із ключових елементів у рамках запропонованої концепції ЦСЕ. Висновок експерта у такому випадку трансформує розрізнені технічні дані у цілісну фактичну картину, що є необхідною для доказування у кримінальному провадженні.

Прийняття та реалізація Single Programming Document 2026-2028 [6] Європейського органу з питань боротьби з відмиванням коштів (AMLA) закладає нормативну та технологічну основу для переходу від традиційної перевірки паперових носіїв до високотехнологічного аналізу цифрових екосистем даних. Зокрема, створення єдиного AML/CFT Rulebook, формування централізованої бази даних та впровадження AI/ML-аналітики забезпечують експертам нові інструменти для ідентифікації, аналізу та інтерпретації цифрових економічних доказів. Участь експертів у сфері криптоактивів у спільних аналітичних розслідуваннях підрозділів фінансової розвідки (Financial Intelligence Units, FIU), а також у процесах нагляду за фінансовим і нефінансовим секторами, розширює їхню роль у виявленні схем відмивання коштів, фінансування тероризму та обходу санкцій.

Перспективи розвитку судово-економічної експертизи у 2026 році визначаються глибокою кореляцією між стандартами оперативної стійкості (DORA) та новими регуляторними стандартами AMLA. Делеговані регламенти[1] (ЄС) 2025/1190 [15] та (ЄС) 2025/532 [16], ухвалені в межах DORA, фіксують вимоги до технічної інфраструктури та процедур тестування на проникнення (TLPT), тоді як майбутні регуляторні технічні стандарти (RTS) AMLA деталізують протоколи звітності та ідентифікації підозрілих операцій [17]. Таким чином, стандарти DORA та AMLA у взаємодії формують технічну та аналітичну основу для оцінки цифрових доказів. За умови надання відповідної документації в процесуальному порядку, експерт може обґрунтовано посилатися на порушення стандартів ІКТ-безпеки (за DORA) як на непрямий доказ свідомого створення умов для приховування фінансових злочинів (за AMLA), що значно посилює обґрунтованість експертного висновку.

Прикладом актуальності і доцільності таких підходів є також і той факт, що після лютого 2022 року ринок російських криптобірж зазнав стрімкої трансформації. Близько 95% з них тепер класифікуються як високоризикові, що є не випадковим збігом, а прямим наслідком їхньої адаптації до нових реалій. Ці платформи перетворилися на тіньову фінансову інфраструктуру, що цілеспрямовано використовується для фінансування війни в умовах, коли легальні фінансові шляхи заблоковані міжнародними санкціями [18].

Ефективне розслідування економічних злочинів у воєнний час, особливо транснаціональних схем, вимагає перегляду методологічних засад судово-економічної експертизи. Дане зумовлене, крім іншого, проблемою інформаційної перенасиченості. Згідно з прес-релізом Європейської комісії від 14 квітня 2021 року, до 80% злочинів мають цифровий компонент [19]. Тому, інтеграція інструментів ШІ та машинного навчання у методологічну базу ЦСЕ є оперативною вимогою. Ці інструменти дозволяють автоматизувати та пришвидшити обробку фінансової інформації, а також виявлення аномалій, притаманних тіньовим операціям. ШІ може використовуватися для мережевого аналізу, виявлення прихованих зв’язків між компаніями-прокладками та оцінки ризиків, пов’язаних із бенефіціарним володінням.

Крім того, сучасна практика судово-економічної експертизи стикається з процесуальними викликами на межі економіки та цифрової криміналістики.

[1] нормативні акти Європейської комісії, що деталізують і доповнюють положення базових регламентів Європейського Парламенту

Кримінальний процесуальний кодекс України та Закон України “Про судову експертизу” поки що не містять уніфікованих стандартів роботи з цифровими економічними доказами. Це створює практичну потребу у розробці чітких процедур збору, збереження та автентифікації цифрових даних, зокрема блокчейн-транзакцій, log-файлів та результатів роботи алгоритмів штучного інтелекту, у спосіб, що забезпечує їх процесуальну допустимість у кримінальному провадженні.

У цьому контексті європейський досвід, закріплений у стандартах AMLA та DORA, демонструє можливість інтеграції цифрової криміналістики у судово-економічну експертизу. Вимоги до кіберстійкості інфраструктури (DORA) та протоколи звітності й ідентифікації підозрілих операцій (AMLA) формують методологічну основу для того, щоб експерт міг не лише аналізувати фінансові дані, але й підтверджувати їхню автентичність та достовірність у процесуальному вимірі. Таким чином, цифрова судово-економічна експертиза постає як міждисциплінарна сфера, що поєднує економічні знання з інструментарієм цифрової криміналістики, забезпечуючи науково обґрунтовану інтерпретацію цифрових доказів у справах про фінансові злочини.

В Україні вже розпочато дискусію щодо поступового визнання нових цифрових доказів у кримінальному процесі. Юристи активно аналізують положення Регламенту ЄС MiCA (Markets in Crypto-Assets Regulation), який встановлює правила для ринку криптоактивів та визначає стандарти прозорості й автентичності транзакцій у блокчейні. Саме на прикладі MiCA формується модель гармонізації українського законодавства з європейськими нормами, зокрема блокчейн-записи розглядаються як потенційно належні юридичні докази, що потребують адаптації процесуальних процедур збору та збереження [20].

Водночас питання інтеграції стандартів AMLA поки що перебуває на етапі очікування, але є очевидним, що після завершення розробки регуляторних технічних стандартів (RTS) у 2026 році вони стануть наступним кроком у формуванні єдиної системи цифрової судово-економічної експертизи. Показовим у цьому контексті є дослідження експертів Вроцлавського університет економіки та бізнесу [21], у якому Україна розглядається як держава з унікальним поєднанням високого рівня використання криптоактивів та активного процесу адаптації національного законодавства до стандартів ЄС. Автори підкреслюють, що на відміну від країн Вишеградської групи, де механізми роботи з цифровими фінансовими даними вже частково інституціоналізовані, в Україні ці процеси перебувають на стадії формування, що створює передумови для апробації нових моделей судово-економічної експертизи. Поєднання європейських AML-стандартів із національними процесуальними нормами відкриває можливість переходу від фрагментарного аналізу окремих транзакцій до комплексного дослідження цифрових економічних слідів, зокрема блокчейн-даних, криптовалютних потоків та пов’язаних із ними ризиків відмивання коштів. У цьому сенсі Україна постає як держава з унікальними передумовами для апробації та впровадження нових моделей судово-економічної експертизи, орієнтованих на інтеграцію європейських регуляторних підходів з національними процесуальними нормами.

Що ж стосується безпосередньо діяльності експертів, то формування чіткої, прикладної структури спеціальних кіберекономічних знань випливає з необхідності систематизувати різнорідні компетенції, що сьогодні залучаються до розслідування цифрових фінансових правопорушень. Аналіз нормативних ініціатив ЄС та методологічні вимоги до доказовості вказують на те, що ці компетенції природно групуються за функціональними підходами:

1) *економічно-фінансовий аналіз* (оцінка економічного змісту операцій і ризик-фреймворків). Згадані нами ініціативи AMLA закладають створення єдиної "data-ecosystem", уніфікацію форматів звітності та розробку загальноєвропейських risk-frameworks. Це забезпечує передумови для порівняльного економічного аналізу транзакцій, стандартизації метаданих і побудови спільних аналітичних інструментів FIU; для експерта буде можливість оперувати уніфікованими наборами даних і застосовувати порівняльні моделі ризику;

2) *криміналістично-технічні процедури* (відновлення та забезпечення цілісності цифрових слідів). DORA та делеговані акти, що регламентують TLPT і управління ICT-субпідрядниками, встановлюють критерії оцінки цілісності цифрової інфраструктури і процедури тестування на проникнення. Це підґрунтя для формалізації аудиту цифрових слідів, визначення критеріїв їхньої надійності та розробки стандартів збереження ланцюга зберігання доказів. Для криміналістичної частини СКЕЗ є необхідністю інтеграції TLPT-сумісності та аудиту ICT-субпідряду у протоколи прийому й перевірки цифрових доказів;

3) *аналітика даних і алгоритмічна верифікація* (кластеризація, ML/AI-валідація, метадані). Застосування алгоритмічного навчання та штучного інтелекту у фінансовому моніторингу вимагає прозорих підходів до валідації, версіонування моделей і метрик якості. AMLA і суміжні ініціативи ЄС акцентують увагу на стандартах метаданих і інструментах для спільної аналітики FIU, що дозволяє узгодити підходи до тестування кластеризацій, скорингових моделей і алгоритмічних висновків; для експерта це означає обов'язок документувати версії, параметри, метрики і тести відтворюваності;

4) *процесуальні механізми* (правовий статус активів, доступ до off-chain джерел, процесуальне документування). MiCA встановлює класифікацію криптоактивів і обов'язки постачальників послуг з криптоактивами (CASP), що впливає на доступність off-chain джерел (KYC, реєстри транзакцій) і на правовий статус об'єктів дослідження. Чітка класифікація активів полегшує визначення предмета експертизи, а регламентація обов'язків CASP створює процесуальні підстави для отримання необхідних підтверджень у кримінальних провадженнях.

Прийняття та поетапна реалізація нових стандартів Європейського Союзу у сферах AML/CFT, цифрової операційної стійкості та регулювання криптоактивів створює підґрунтя для переосмислення підходів до цифрових економічних доказів у кримінальному провадженні. У цьому контексті AMLA, DORA та MiCA слід розглядати не лише як регуляторні акти фінансового чи технічного характеру, а і як джерело нормативних орієнтирів для формування сучасної моделі роботи з цифровими даними, які можуть набувати доказового значення.

Зокрема, стандарти AMLA закладають основу для уніфікації підходів до виявлення, документування та аналітичної оцінки підозрілих фінансових операцій, у тому числі тих, що здійснюються з використанням криптоактивів. Розвиток єдиного AML/CFT Rulebook, побудова централізованої екосистеми даних та впровадження AI/ML-аналітики у сфері фінансового моніторингу створюють передумови для стандартизації тих інформаційних масивів, які в подальшому можуть використовуватися як джерело цифрових економічних доказів.

DORA, своєю чергою, формує важливу нормативну рамку для оцінки надійності цифрової інфраструктури, цілісності інформаційних систем та стійкості фінансових суб'єктів до кіберризиків. Для кримінального провадження це має значення остільки, оскільки цифрові економічні докази не можуть оцінюватися ізольовано від умов їх виникнення, обробки, збереження та передачі. Питання цілісності цифрового

середовища, ланцюга зберігання даних, надійності журналів подій, результатів тестування систем і процедур контролю доступу безпосередньо впливають на достовірність і відтворюваність цифрових слідів, які надалі стають предметом експертного дослідження.

Не менш важливе значення має MiCA, яка встановлює правовий режим криптоактивів і діяльності постачальників послуг, пов'язаних із ними. Саме цей регламент створює більш визначені правові рамки для класифікації цифрових активів, встановлення статусу учасників ринку, а також доступу до off-chain джерел інформації, зокрема KYC/AML-документації, реєстраційних та транзакційних даних. У площині кримінального провадження це посилює можливості правової ідентифікації цифрових економічних доказів та їх співвіднесення з конкретними суб'єктами, активами й фінансовими операціями.

Для України значення цих підходів є подвійним. З одного боку, держава перебуває у процесі адаптації законодавства до права ЄС та формування сучасної моделі регулювання криптоактивів і цифрових фінансових ринків. З іншого боку, саме українська практика особливо гостро стикається з ризиками використання цифрових платформ, віртуальних активів і децентралізованих інструментів для обходу санкцій, приховування активів, фінансування терористичної та диверсійної діяльності. За таких умов цифрові економічні докази мають розглядатися не як вузькоспеціальний технічний феномен, а як важливий елемент системи кримінального доказування, що потребує окремого правового, організаційного та експертного опрацювання.

У цьому сенсі адаптація європейських підходів до української правозастосовної практики має охоплювати не лише імплементацію окремих регуляторних норм, а і розробку процедур збирання, збереження, верифікації, автентифікації та експертної інтерпретації цифрових економічних доказів. Особливої уваги потребують питання стандартизації методик блокчейн-аналітики, документування алгоритмічних висновків, перевірки відтворюваності результатів AI/ML-аналізу, а також забезпечення процесуальної допустимості матеріалів, що поєднують on-chain і off-chain джерела інформації.

Таким чином, стандарти AMLA, DORA та MiCA можуть розглядатися як комплексне підґрунтя для формування в Україні нової моделі роботи з цифровими економічними доказами, у межах якої поєднуються правові, криміналістичні, технологічні та економічні підходи. Саме така модель відповідає сучасним викликам фінансової злочинності й відкриває перспективи для підвищення якості доказування у кримінальному провадженні.

Висновки. У результаті проведеного дослідження встановлено, що цифровізація фінансової злочинності зумовила появу нового масиву доказової інформації, який потребує окремого правового та експертного осмислення у кримінальному провадженні. Блокчейн-записи, on-chain та off-chain дані, log-файли, відомості фінансового моніторингу, результати алгоритмічного аналізу та інші цифрові сліди вже сьогодні відіграють істотну роль у справах про відмивання коштів, обхід санкцій, фінансування терористичної діяльності та інші форми економічної злочинності. У зв'язку з цим цифрові економічні докази доцільно розглядати як особливий різновид цифрової доказової інформації, правове значення якої формується на перетині кримінального процесу, фінансового моніторингу, цифрової криміналістики та регулювання криптоактивів.

Доведено, що основна проблема у роботі з цифровими економічними доказами полягає не лише у виявленні цифрових слідів, а у забезпеченні їх належної верифікації,

автентифікації, відтворюваності та процесуальної інтерпретації. Саме тому дослідження таких доказів потребує міждисциплінарного підходу, що поєднує економічний аналіз, блокчейн-аналітику, цифрову криміналістику, роботу з даними та, за необхідності, інструменти штучного інтелекту і машинного навчання.

Обґрунтовано доцільність використання категорії "спеціальні кіберекономічні знання" для позначення комплексу компетенцій, необхідних для роботи з цифровими економічними доказами у кримінальному провадженні. У межах цього підходу цифрову судово-економічну експертизу запропоновано розглядати як перспективну процесуально-експертну модель дослідження цифрових економічних доказів, спрямовану на встановлення їх економічного змісту, технічної достовірності та юридичної релевантності.

Встановлено, що досвід Європейського Союзу, насамперед у межах AMLA, DORA та MiCA, формує важливі орієнтири для побудови сучасної системи роботи з цифровими економічними доказами. AMLA задає стандарти уніфікації AML/CFT-підходів і розвитку data-driven та AI/ML-орієнтованої аналітики; DORA створює нормативну основу для оцінки цілісності цифрової інфраструктури та надійності цифрових джерел; MiCA забезпечує правову визначеність у сфері криптоактивів і доступу до off-chain інформації. У сукупності ці акти формують методичне підґрунтя для подальшого розвитку процедур верифікації, документування та процесуального використання цифрових економічних доказів.

Для України адаптація зазначених підходів має не лише євроінтеграційне, а й безпекове значення. В умовах війни, санкційного тиску та активного використання криптоактивів у схемах приховування фінансових потоків формування сучасної моделі роботи з цифровими економічними доказами є практичною необхідністю. Перспективними напрямами подальшого розвитку слід вважати розробку уніфікованих процедур збору та збереження цифрових економічних доказів, стандартизацію методик блокчейн-аналітики, документування результатів AI/ML-аналізу, а також удосконалення процесуальних підходів до оцінки допустимості та доказової сили таких матеріалів у кримінальному провадженні.

Отже, цифрові економічні докази мають розглядатися як один із ключових об'єктів сучасного кримінального доказування у справах про фінансові злочини. Їх ефективне використання можливе лише за умови поєднання правових, експертних і технологічних підходів, здатних забезпечити науково обґрунтоване перетворення цифрових слідів на належну й допустиму доказову інформацію.

ПОДЯКИ: Немає
КОНФЛІКТ ІНТЕРЕСІВ: Немає

Використана література

1. Crypto Crime Reaches Record High in 2025 as Nation-State Sanctions Evasion Moves On-Chain at Scale. Report. 08.01.2026 https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/

2. The changing DNA of serious and organised crime. EU Serious and Organised Crime Threat Assessment 2025 (EU-SOCTA). Europol. 27.05.2025 URL: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf .

3. Gonzalo Saiz Erausquin Reassessing the Financing of Terrorism in 2025. RUSI. 11.09.2025 URL: https://www.rusi.org/explore-our-research/publications/insights-papers/reassessing-financing-terrorism-2025.

4. Hugo Grimbel du Bois, Anne Hyvernaud European Anti-Financial Crime Executive Priorities For 2026. Oliver Wyman https://www.oliverwyman.com/our-expertise/insights/2026/feb/european-anti-financial-crime-transformation-2026.html

5. The Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) URL: https://www.amla.europa.eu/index_en

6. Single Programming Document 2026-2028. AMLA. 04.02.2026 URL: https://www.amla.europa.eu/document/download/27549516-d110-4e91-b1ed-d3552b8f9661_en?filename=AMLA+SPD+2026-2028.pdf&utm_source=copilot.com

7. Шепітько В. Ю. Криміналістика. Енциклопедичний словник (українсько-російський і російсько-український) / за ред. акад. В. Я. Тація. Харків: Право, 2001. 560 с.

8. Експертизи у судовій практиці: підручник / за заг. ред. В. Г. Гончаренка. Київ: Юрінком Інтер, 2004. 388 с.

9. Горлачук О. До питання про спеціальні знання судового експерта-економіста. Теорія та практика судової експертизи і криміналістики. 2021. Випуск 2 (24) URL: https://khrife-journal.org/index.php/journal.

10. Тактика проведення судових експертиз: метод. рек. / укл. М. Г. Щербаковський. Харків: Нац. ун-т внутр. справ, 2004. 60 с.

11. Paul Reedy Interpol review of digital evidence 2016 – 2019. Forensic Science International: Synergy. Volume 2, 2020, Pages 489-520 URL: https://pdf.sciencedirectassets.com/319960/1-s2.0-S2589871X19X00054/1-s2.0-S2589871X20300152/main.pdf.

12. Leveraging modern technology for swift, targeted digital investigations of financial crime. Moody's Apr 24, 2025 URL: https://www.moodys.com/web/en/us/kyc/resources/insights/leveraging-modern-technology-digital-investigations-financial-crime.html.

13. Noelle Hartt What Is Digital Forensics? When IT Meets Criminal Justice. Criminal Justice Blog. American Military University. 20.02.2025 URL: https://www.amu.apus.edu/area-of-study/criminal-justice/resources/what-is-digital-forensics-in-criminal-justice/.

14. Joel Khalili The Science of Crypto Forensics Survives a Court Battle—for Now. Wired. 27.03.2024 URL: https://www.wired.com/story/the-science-of-crypto-forensics-court-battle/

15. Commission Delegated Regulation (EU) 2025/1190 of 13 February 2025 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria used for identifying financial entities required to perform threat-led penetration testing, the requirements and standards governing the use of internal testers, the requirements in relation to the scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition: Document 32025R1190 URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R1190

16. Commission Delegated Regulation (EU) 2025/532 of 24 March 2025 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the elements that a financial entity has to determine and assess when subcontracting ICT services supporting critical or important functions. Document 32025R0532 URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0532

17. Regulatory Instruments. AMLA. 16.12.2025 URL: https://www.amla.europa.eu/policy/regulatory-instruments_en?utm_source=copilot.com

18. Treasury Designates Russian Companies Supporting Sanctions Evasion Through Virtual Asset Services and Technology Procurement. U.S. Department of the Treasury. 25.03.2024 URL: https://home.treasury.gov/news/press-releases/jy2204

19. Fight against organised crime: New 5-year strategy for boosting cooperation across the EU and for better use of digital tools for investigations. European Commission. Apr 14, 2021 URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1662

20. Шевчук О. Реалістичний шлях законодавчого визнання блокчейн-запису як належної юридичної підстави. Національна асоціація лобістів України. 18.01.2026 URL:

https://unla.org.ua/2026/01/realistychnyj-shlyah-zakonodavchogo-vyznannya-blokchejn-zapysu-yak-nalezhnoyi-yurydychnoyi-pidstavy/

21. Bartłomiej Nita Blockchain Technology in Anti-Money Laundering: Challenges and Opportunities in the V4 Countries and Ukraine. Publishing House of Wroclaw University of Economics and Business. 2025. URL: https://dbc.wroc.pl/Content/133768/Nita_Blockchain_Technology_in_Anti-Money_Laundering.pdf?utm_source=copilot.com

Олександр Дмитрович Довгань
заслужений діяч науки і техніки, доктор юридичних наук, професор
радник дирекції Державної наукової установи "Інститут інформації, безпеки і права Національної академії правових наук України"
04053, Україна, м. Київ, пров. Несторівський, 4
email: dod16.67@ukr.net
Тарас Юрійович Ткачук
доктор юридичних наук, професор
учений секретар наукової лабораторії (наукової установи) Українського науково-дослідного інституту спеціальної техніки та судових експертиз
03113, Україна, м. Київ, вулиця Миколи Василенка, 3
email: tarast25@gmail.com
Віталій Геннадійович Оніщенко
провідний науковий співробітник наукової лабораторії (наукової установи) Українського науково-дослідного інституту спеціальної техніки та судових експертиз
03113, Україна, м. Київ, вулиця Миколи Василенка, 3
email: nauka_icte@ssu.gov.ua

Oleksandr D. Dovhan
Merited Figure of Science and Technology of Ukraine, Doctor of Juridical Sciences, Professor
Adviser to the Directorate of the State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
04053, Ukraine, Kyiv, Nestorivskyi Lane, 4
email: dod16.67@ukr.net
Taras Yu. Tkachuk
Doctor of Juridical Sciences, Professor
Academic Secretary of the Scientific Laboratory (Scientific Institution) of the Ukrainian Scientific Research Institute of Special Equipment and Forensic Examinations
03113, Ukraine, Kyiv, Mykola Vasylenko Street, 3
email: tarast25@gmail.com
Vitalii H. Onishchenko
Leading Research Fellow of the Scientific Laboratory (Scientific Institution) of the Ukrainian Scientific Research Institute of Special Equipment and Forensic Examinations
03113, Ukraine, Kyiv, Mykola Vasylenko Street, 3
email: nauka_icte@ssu.gov.ua

Рекомендоване цитування: Довгань О.Д., Ткачук Т.Ю., Оніщенко В.Г. Цифрові економічні докази у кримінальному провадженні: правові та експертні підходи крізь призму стандартів ЄС. *Інформація і право*. № 2(57)/2026. 2026. С. 282-296. https://doi.org/10.37750/2616-6798.2026.2(57).364550

Suggested Citation: Dovhan O., Tkachuk T., Onishchenko V. (2026) Digital Economic Evidence in Criminal Proceedings: Legal and Expert Approaches Through the Prism of EU Standards. *Information and Law*. 2(57)/2026. 282-296. https://doi.org/10.37750/2616-6798.2026.2(57).364550

Дата надходження статті до редакції: 21.04.2026 р.
Дата прийняття статті до друку після рецензування: 29.04.2026 р.
Дата публікації (оприлюднення): 31.05.2026 р.

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