УДК 343.1
DOI https://doi.org/10.32782/2524-0374/2025-2/151

РОЛЬ ЦИФРОВИХ ДОКАЗІВ ПІД ЧАС РОЗСЛІДУВАННЯ ЕКОНОМІЧНИХ ЗЛОЧИНІВ

THE ROLE OF DIGITAL EVIDENCE IN THE INVESTIGATION OF ECONOMIC CRIMES

Кутепов І.О., аспірант заочної форми навчання докторантури та аспірантури
Одеський державний університет внутрішніх справ

Стрімка цифровізація економіки, зростання обсягів електронних фінансових операцій, поширення криптовалют та віртуальних активів, а також глобальна інтеграція бізнес-процесів зумовили радикальні зміни у природі вчинення, організації та приховування економічних злочинів. Злочинна діяльність у сфері легалізації доходів, ухилення від сплати податків, фальсифікації фінансової звітності або маніпулювання платіжними інструментами дедалі частіше реалізується із використанням новітніх цифрових технологій, а отже, потребує адекватних правових і процесуальних засобів реагування.

У цьому контексті особливого значення набуває цифрове доказування – тобто фіксація, аналіз і використання в межах кримінального провадження інформації, зафіксованої в електронній формі та здобутої з комп'ютерних систем, цифрових пристроїв, інформаційних мереж, хмарних платформ, реєстрів або криптоінфраструктури.

Саме цифрові сліди – журнали операцій, IP-логування, блокчейн-транзакції, файли бухгалтерських систем, криптовалютні гаманці, електронний документообіг тощо – все частіше є єдиним можливим шляхом доведення вчинення злочинного діяння в умовах, коли класичних слідів правопорушення може не існувати. Разом із тим, правозастосовна практика в Україні стикається з рядом викликів, пов'язаних із використанням цифрових доказів у справах економічного характеру. Відсутність чіткої дефініції цифрових доказів у Кримінальному процесуальному кодексі України, нечіткий статус даних, отриманих з відкритих джерел (OSINT), проблеми фіксації цифрових слідів відповідно до вимог допустимості, обмеженість технічної експертизи, а також юрисдикційна розмитість розміщення цифрових об'єктів – усе це суттєво ускладнює ефективне розслідування та притягнення до відповідальності за економічні злочини у цифровому середовищі.

У зв'язку з цим виникає необхідність наукового переосмислення місця та ролі цифрових доказів у системі доказування, зокрема – в економічних кримінальних провадженнях. Це вимагає як аналітичного дослідження правової природи цифрових доказів, їх джерел і процесуальних особливостей, так і формування обґрунтованих пропозицій щодо вдосконалення національного кримінального процесуального законодавства, імплементації міжнародних стандартів та розробки відповідної методології цифрової криміналістики.

Метою цієї статті є висвітлення ключових проблем теоретико-практичного характеру, пов'язаних із використанням цифрових доказів у розслідуванні економічних злочинів, та окреслення перспектив законодавчого й інституційного розвитку відповідної сфери в умовах цифрової доби.

Ключові слова: цифрові докази, економічні злочини, OSINT, електронні сліди, цифрова криміналістика, допустимість доказів.

The rapid digitalization of the economy, the growth of electronic financial transactions, the proliferation of cryptocurrencies and virtual assets, and the global integration of business processes have led to radical changes in the nature of economic crimes, their organization and concealment. Criminal activities in the area of money laundering, tax evasion, falsification of financial statements or manipulation of payment instruments are increasingly being carried out using the latest digital technologies and, therefore, require adequate legal and procedural responses.

In this context, digital evidence, i.e., the recording, analysis and use of information recorded in electronic form and obtained from computer systems, digital devices, information networks, cloud platforms, registries or crypto-infrastructure within criminal proceedings, is of particular importance

It is digital traces - transaction logs, IP logging, blockchain transactions, accounting system files, cryptocurrency wallets, electronic document flow, etc. - that are increasingly the only possible way to prove a criminal act in circumstances where classic traces of an offense may not exist. At the same time, law enforcement practice in Ukraine faces a number of challenges related to the use of digital evidence in economic cases. The absence of a clear definition of digital evidence in the Criminal Procedure Code of Ukraine, the unclear status of open source intelligence (OSINT), problems with capturing digital traces in accordance with the admissibility requirements, limited technical expertise, and jurisdictional blurring of the location of digital objects all significantly complicate the effective investigation and prosecution of economic crimes in the digital environment.

In this regard, there is a need for a scientific rethinking of the place and role of digital evidence in the system of evidence, in particular, in economic criminal proceedings. This requires both an analytical study of the legal nature of digital evidence, its sources and procedural features, and the development of reasonable proposals for improving national criminal procedure legislation, implementing international standards and developing an appropriate digital forensics methodology.

The purpose of this article is to highlight the key theoretical and practical issues related to the use of digital evidence in the investigation of economic crimes and to outline the prospects for legislative and institutional development of the relevant area in the digital age.

Key words: digital evidence, economic crimes, OSINT, electronic traces, digital forensics, admissibility of evidence.

Виклад основного матеріалу. У сучасних умовах цифрової трансформації економіки та правової системи, використання цифрових доказів набуває ключового значення у розслідуванні кримінальних правопорушень економічного характеру.

Згідно з положеннями статті 84 Кримінального процесуального кодексу України, доказами визнається будь-яка фактична інформація, що має значення для кримінального провадження, здобута у передбаченому законом порядку [1].

Авдєєва Г. визначає цифрові докази як фактичні дані, які представлені у вигляді бінарного (двійкового) коду та містять інформацію, що має значення для об'єктивного вирішення справи [2, с. 131].

Дослідники кримінального процесу визначають електронні докази як об'єкти цифрового (електронного) виміру, що можуть мати значення для кримінального провадження. Фігурський В. М. зазначає, що докази в електронній формі – це інформація, створена, оброблена, збережена або передана за допомогою аналогових чи цифрових сигналів, що має значення для кримінального провадження [3, с. 99].

Отже, цифрові докази – це інформація, зафіксована в електронній (нематеріальній) формі, що міститься в комп'ютерних системах, цифрових пристроях, мобільних додатках, інформаційних мережах або хмарних середовищах, яка може бути використана для встановлення обставин вчинення злочину, зокрема – у справах щодо легалізації доходів, ухилення від сплати податків, шахрайства, зловживань у банківській сфері, маніпуляцій з фінансовою звітністю тощо.

Цифрові докази мають низку характерних особливостей, що відрізняють їх від традиційних (матеріальних чи документальних) джерел доказування. Насамперед, йдеться про нематеріальну природу такого роду даних, їх залежність від технічного середовища, можливість знищення або модифікації без фізичного втручання, а також

транскордонний характер зберігання, що ускладнює доступ до відповідної інформації без міжнародного співробітництва.

Колодіна А. С. зазначає, що у порівнянні з традиційними доказами, цифрові докази створюють унікальні складності при аутентифікації через обсяг доступних даних, їх швидкості, нестійкості та вразливості (легко можуть бути змінені та/або знищені). Аутентифікація цифрових доказів має важливе значення, адже перш ніж цифрові докази можуть бути представлені в суді в якості прямих або непрямих доказів, їх треба розпізнати [4, с. 179].

Як зазначають Гуцалюк М. В. та П. Є. Антонюк, інформація, зафіксована в електронній (цифровій) формі, може легко змінюватися, знищуватися, передаватися, копіюватися. Специфічна природа інформації в електронному вигляді полягає в тому, що вона є доступною для сприйняття людиною не безпосередньо, а тільки після обробки її спеціальними програмними засобами, які, у свою чергу, функціонують під управлінням операційної системи на певному комп'ютерному пристрої. Тобто, перегляд різними програмними засобами фізично однакової інформації у вигляді бітів (мінімальна одиниця кількості інформації) на жорсткому диску призведе на екрані монітору чи роздруківці принтеру до різного виду фактичних даних [5, с. 118].

Значна частина цифрових доказів, зокрема у справах економічної спрямованості, розміщується у віддалених дата-центрах, хмарних сховищах або серверних фермах, контроль над якими можуть мати суб'єкти, що перебувають поза межами національної юрисдикції. Це створює додаткові виклики щодо витребування, фіксації та процесуальної допустимості таких доказів у межах національного кримінального провадження.

Крім того, цифрові сліди часто є вторинними або похідними: вони можуть бути створені не безпосередньо злочинцем, а в результаті його дій – наприклад, записи логів доступу до фінансових систем, зміни у бухгалтерських базах даних, запити до серверів платіжних шлюзів або дії, пов'язані із запуском шкідливого програмного забезпечення. Як зазначає Полотай О. І., існують активні та пасивні цифрові сліди. Активні цифрові сліди створюються на основі даних, наданих користувачем, таких як персональні дані, відео, зображення та коментарі, розміщені в додатках, веб-сайтах, соціальних мережах тощо. Пасивні цифрові сліди – дані, ненавмисно залишені людьми, які використовують мережу Інтернет або цифрові технології [6, с. 77-78].

У випадках, коли йдеться про легалізацію доходів, отриманих злочинним шляхом, цифрові докази дозволяють встановити структуру транзакцій, зв'язки між суб'єктами господарювання, електронний документообіг, участь у криптовалютних операціях тощо. Водночас виникає низка складних процесуальних запитань: які саме сліди можуть бути кваліфіковані як докази? Чи можуть логи податкових сервісів, експортовані у форматі JSON або XML, бути визнані повноцінним процесуальним доказом? Як забезпечити незмінність хеш-функції цифрового файлу? Чи допустимо отримувати цифрові дані поза межами кримінального провадження через процедури OSINT або технічну експертизу? Саме ці проблеми формують підґрунтя для глибшого аналізу правової природи цифрових доказів та пошуку належного механізму їх нормативної регламентації в умовах стрімкого розвитку економічної кіберзлочинності.

Open Source Intelligence (OSINT) – це розвідка на основі відкритих джерел, яка передбачає збір, аналіз і використання інформації з публічно доступних джерел в інтернеті, зокрема веб-сайтів, баз даних, реєстрів, соціальних мереж, форумів, бірж криптовалют, медіаресурсів та інших цифрових майданчиків. У межах розслідування економічних злочинів OSINT дедалі частіше виступає як додатковий аналітичний інструмент для виявлення зв'язків між суб'єктами, відстеження цифрових транзакцій, верифікації бенефіціарів, ідентифікації офшорних структур та аналізу схем ухилення від оподаткування. Особливу значущість OSINT набуває у випадках, коли основна частина цифрових слідів або економічної активності перебуває поза межами юрисдикції України, наприклад, компанія зареєстрована на Віргінських островах, але бере участь у схемі ПДВ в Україні, або платіжний шлюз розміщено на сервері в Канаді, але його IP-адреса фіксується у тіньовій транзакції.

Завдяки OSINT-аналітиці можуть бути здобуті такі типи цифрової інформації: метадані про доменні імена та хостинги (через сервіси WHOIS, DNS-lookup); цифрові сліди діяльності суб'єктів господарювання в реєстрах (наприклад, OpenCorporates, YouControl, КОАТУУ, ДРФО); історія транзакцій у публічних блокчейнах; аналіз активності осіб у соціальних мережах (через Graph API, Maltego, або OSINT Toolkits); виявлення повторюваних шаблонів діяльності на торговельних та краудфандингових платформах; аналіз кодування та сертифікатів у фінансових документах, опублікованих в мережі.

Однак з процесуальної точки зору OSINT не завжди визнається повноцінним доказом у кримінальному провадженні, оскільки джерело такої інформації не завжди є надійним, а спосіб її здобуття – не завжди відповідає нормам Кримінального процесуального кодексу України.

Наприклад, самостійно отриманий скріншот з веб-сайту або збережена копія сторінки без засвідченого джерела, хеш-підтвердження чи протоколу огляду в режимі фіксації (наприклад, з використанням програми «WebPreserver») можуть бути визнані неналежним доказом. Тому OSINT-дані переважно мають аналітичне значення – як джерело орієнтувальної або попередньої інформації для формування версій, обґрунтування підстав для клопотання про обшук, тимчасовий доступ або експертизу.

У деяких випадках така інформація може бути використана в ході слідчих (розшукових) дій, але з обов'язковим процесуальним закріпленням: наприклад, у вигляді протоколу огляду вебресурсу з технічним фіксуванням, залученням спеціаліста та створенням цифрового слепшоту (snapshot) із хеш-сертифікацією. Крім того, низка країн і міжнародних організацій розробляють стандарти допустимості OSINT-даних як доказів у кримінальному провадженні.

Збирання та використання доказів, отриманих з відкритих джерел, за загальним правилом, має здійснюватися за протоколом Берклі. Так, щодо інформації з відкритих джерел протоколом Берклі рекомендовано фіксувати щонайменше такі дані: цільова вебадреса; вихідний код; захоплення всієї вебсторінки або зображення повідомлення крауд-месенджера в застосунку; вбудовані мультимедійні файли; вбудовані метадані; контекстуальні дані; хеш-значення; дані про процес збирання інформації [7, с. 110].

Наприклад, у практиці правоохоронних органів Німеччини, Великобританії та США OSINT-фрагменти можуть входити до складу доказової бази за умови дотримання стандартів chain of custody (ланцюга збереження доказів) та цифрової фіксації із зазначенням джерела, дати та умов отримання.

Таким чином, у сфері розслідування економічних злочинів OSINT може виступати як ефективний засіб: побудови гіпотез і аналітичних моделей злочинної діяльності; ідентифікації цифрових слідів і потенційних суб'єктів злочину; доповнення цифрових доказів, отриманих у процесуальний спосіб; збирання інформації для подальших процесуальних рішень. Водночас його правове значення обмежене рамками чинного процесуального регулювання, що актуалізує необхідність законодавчої деталізації статусу відкритих цифрових джерел у кримінальному процесі України.

Цифрові докази у кримінальному провадженні щодо економічних злочинів можуть походити з різноманітних джерел, які функціонують як у межах юрисдикції України, так і за її межами. Особливість цих джерел полягає у тому, що вони відображають не лише факт вчинення дії, а й цифрові сліди процесів, які безпосередньо стосуються походження, руху та маскування злочинних активів. Саме тому джерела цифрових доказів в економічній сфері є ключовими для побудови доказової бази у справах про ухилення від оподаткування, легалізацію доходів, маніпуляції з фінансовою звітністю, злочини у сфері банківських послуг та криптовалютного обігу. Найбільш поширеними джерелами цифрових доказів у справах економічного спрямування є інформаційно-аналітичні системи підприємств і фінансових установ. Зокрема, йдеться про бухгалтерські програми, системи електронного документообігу (M.E.Doc, Document.online), електронні банкінги, внутрішньокорпоративні сервери, поштові платформи тощо. У таких джерелах зберігаються як дані про первинні документи (рахунки, акти, накладні), так і інформація про зміну та обробку цих документів (метадані, IP-адреси, хронологія редагування, авторизація користувачів). Іншим важливим джерелом цифрової доказової інформації виступають державні та відкриті реєстри, зокрема Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців, Єдиний реєстр податкових накладних, Єдиний державний реєстр судових рішень, системи «Прозоро», реєстр речових прав тощо. За допомогою аналітичних інструментів (YouControl, Opendatabot, Ring, CBR) можливо реконструювати ланцюг зв'язків між фіктивними суб'єктами, виявити спроби змінити бенефіціара, відстежити аномальні трансакції або діяльність «сплячих» компаній, залучених до схем податкового планування.

У контексті криптовалют і віртуальних активів важливим джерелом виступають блокчейн-експлорери (наприклад, Etherscan, Blockchair, BscScan), які дозволяють відстежити публічні транзакції, визначити взаємозв'язки між гаманцями, оцінити обсяг незаконного обігу. Хоча інформація в таких системах є відкритою, її процесуальне використання вимагає технічної верифікації (через експертні висновки, хеш-ідентифікацію, сертифікацію цифрових слідів). У справах міжнародного характеру ключову роль відіграють хмарні сервіси, які зберігають значні обсяги бізнес-даних: Google Drive, Dropbox, Amazon Web Services, Microsoft 365 тощо.

Інформація про контракти, платежі, обмін повідомленнями, збереження інвойсів, фінансових таблиць або аудиторських звітів може бути доступною виключно через процедуру міжнародної правової допомоги (MLAT), або ж добровільну передачу даних власником акаунта. У багатьох випадках злочинці використовують ці платформи для зберігання «чистих» версій підроблених документів або для маскування транскордонних операцій між підконтрольними компаніями.

Особливе місце займають також електронні поштові сервіси, корпоративні чати, системи клієнтської підтримки (CRM), які дозволяють відстежити процес обговорення злочинних схем, погодження контрактів, обмін паролями, інструкціями тощо. При цьому дані можуть бути зашифрованими, з обмеженим терміном зберігання, або містити вбудовані елементи антифорензічного захисту (наприклад, самознищувальні повідомлення).

Крім того, значне джерело цифрових слідів становлять інтернет-журнали та логи серверів, що фіксують час входу в систему, геолокацію користувача, параметри сесії, дії в адміністративній панелі, використання VPN або Tor-мереж. Ці дані є особливо цінними для відновлення хронології доступу до файлів, баз даних, банківських сервісів або інтерфейсів обміну криптоактивами.

У кримінальному провадженні щодо економічних злочинів експертиза цифрових доказів є однією з ключових процесуальних гарантій їх допустимості, належності та доказової сили. З огляду на специфіку цифрових даних – їхню нестабільність, змінність, віртуальність і часто – транскордонність – саме експертне дослідження виступає центральним інструментом для встановлення їх автентичності, незмінності, джерела походження та технічної достовірності. Відповідно до положень ст. 101, 242–243 Кримінального процесуального кодексу України, висновок експерта є самостійним видом доказу, який формується на основі спеціальних знань у науці, техніці або інших сферах діяльності [1].

У випадку цифрових доказів такими знаннями виступають знання у сфері інформаційних технологій, комп'ютерної інженерії, цифрової криміналістики, телекомунікацій та криптографії. Зокрема, у процесі експертного дослідження можуть бути вирішені такі ключові завдання: встановлення автентичності цифрових об'єктів – зокрема перевірка хеш-сум, цифрових підписів, наявності ознак редагування файлів; визначення джерела походження даних – ідентифікація IP-адреси, MAC-ідентифікатора, пристрою, з якого здійснено дію; відновлення видалених або модифікованих даних – з використанням методів цифрової реконструкції; встановлення відповідності процедури збору доказів процесуальним вимогам – зокрема, чи дотримано послідовність дій, ланцюг збереження (chain of custody), чи були залучені технічні фіксатори; ідентифікація суб'єкта дій у цифровому середовищі – через поведінковий аналіз, технічні профілі або цифрові сліди.

У справах про ухилення від сплати податків, відмивання коштів, криптовалютне шахрайство або фіктивне підприємництво, саме експертиза дозволяє відокремити достовірну інформацію від потенційно сфальсифікованої або технічно обробленої.

Наприклад, у випадку зміни дати електронного документа або втручання у метадані бухгалтерського файлу, лише експерт може встановити момент втручання, спосіб зміни та технічний інструмент, за допомогою якого це було здійснено. Окремим видом спеціального дослідження виступає експертиза електронної пошти, яка дозволяє виявити не лише вміст повідомлень, а й маршрут їх передачі, використані проксі, час з'єднання, взаємозв'язки між адресатами, факт знищення листів тощо.

У сфері криптовалютних операцій – це експертиза блокчейн-транзакцій, яка передбачає аналіз відкритих блоків, зв'язків між гаманцями, обхід через мікшери (mixer services) або приватні валюти (Monero, Zcash). Не менш важливою є і роль експертизи як гаранта допустимості цифрових доказів у судовому процесі. Адже за відсутності експертного підтвердження автентичності, незмінності та належного способу здобуття, суд вправі визнати такі докази недопустимими. Сучасна правозастосовна практика потребує впровадження стандартизованих методик судової комп'ютерно-технічної експертизи, адаптованих до новітніх цифрових середовищ.

Крім того, варто передбачити можливість створення міжвідомчих експертних центрів з цифрової криміналістики, які поєднуватимуть аналітичний, правовий і технічний потенціал, необхідний для об'єктивної оцінки цифрових слідів.

Допустимість цифрових доказів у кримінальному процесі розглядається в міжнародній правозастосовній практиці як складна багаторівнева проблема, яка потребує синхронізації національних процедур зі світовими стандартами збирання, автентифікації та оцінки електронних даних. В умовах інтенсивного розвитку інформаційно-комунікаційних технологій держави вимушені адаптувати процесуальне законодавство до нової реальності, в якій дедалі більша частина доказової інформації існує в цифровій формі, функціонує у розподілених середовищах та охоплює юрисдикції різних країн.

Електронні докази все частіше стають предметом судової оцінки. У частині випадків електронні докази

можуть вказувати на головний факт вчинення кримінального правопорушення та бути основними в контексті достатності під час прийняття рішення по суті кримінального провадження. Так, оцінюючи можливість використання електронних доказів, зокрема скріншотів у кримінальному судочинстві, Гарасимів О. І., Марко С. І., Ряшко О. В., звертають увагу на судову практику Верховного Суду - постанову у справі № 753/10840/19 від 13 липня 2020 року. У даному випадку Верховний Суд допустив у якості доказу домашнього насильства скріншоти переписки колишньої дружини та чоловіка, в яких останній погрожував їй та дитині, застосовував нецензурні образи, погрози та неприйнятну лексику. Дослідивши надані докази, суд визнав факт домашнього насильства у формі психологічного насильства [8, с. 161].

Також під час розслідування злочинів (наприклад у кіберпросторі) можуть траплятись ситуації де серед доказової бази присутні лише електронні докази.

На рівні Ради Європи ключовим документом, який регламентує міжнародні стандарти щодо електронних доказів, є Конвенція про кіберзлочинність (Будапештська конвенція 2001 року). Вона закладає основи співпраці держав у сфері цифрового доказування, передбачаючи створення національних процедур для фіксації, збереження та правового використання електронної інформації. Країни-учасниці Конвенції на взаємній основі надають один одному можливість отримати максимальну правову допомогу з метою ведення розслідування або судового розгляду у зв'язку з кримінальними правопорушеннями, пов'язаними з комп'ютерними системами та даними, або збору доказів у кримінальному провадженні в електронній формі [9, с. 55].

У 2022 році було прийнято Додатковий протокол до цієї Конвенції, спрямований на подолання викликів, пов'язаних із транскордонним доступом до даних, які зберігаються на серверах в інших країнах. У ньому підкреслено важливість дотримання прав людини, процесуальної справедливості та прозорості механізмів отримання цифрових слідів.

У правових системах Європейського Союзу реалізується концепція взаємного визнання цифрових доказів на базі нормативного комплексу e-Evidence, що інтегрує зусилля країн-членів щодо правової сумісності процесів електронного доказування. Центральним принципом у цьому підході є забезпечення цілісності та автентичності цифрового об'єкта через контроль його походження, фіксацію моменту взаємодії та документування всіх слідчих дій. Високі вимоги встановлюються до технічної експертизи, що має підтвердити незмінність цифрового сліду від моменту його вилучення до подання в суді.

У Сполучених Штатах Америки цифрові докази врегульовані правилами федерального доказового права, зокрема положеннями про автентифікацію. Підхід американських судів ґрунтується на необхідності переконати суд у тому, що цифровий об'єкт є саме тим, за що він подається, а не зміненим чи підробленим артефактом. Таке переконання досягається через спеціалізовану експертизу, застосування криптографічних механізмів фіксації, надійний протокол зберігання об'єкта та контроль доступу до нього.

У Великобританії електронні докази розглядаються в межах законодавства про поліцейську діяльність і кримінальні докази, що встановлює чіткі вимоги до поводження з цифровими носіями. Так, законодавче регулювання електронних доказів регламентується Законом про поліцію та кримінальні докази 1984 р. Згідно ст. 19 вказаного Закону поліція може витребувати будь-яку інформацію, в тому числі в електронній формі. Головна умова полягає в тому, щоб електронна доказова інформація мала відношення до скоєння або запобігання злочинам, а також коли її вилучення сприяє запобіганню приховування, втрати, підробки або знищення доказів у будь-якій формі [10, с.822]. Отже, центральне значення має дотримання презумпції достовірності, яка може бути забезпечена лише за умови технічно грамотно задокументованого вилучення, без змін та зберігання цифрового матеріалу в контрольованому середовищі. Експерт у галузі цифрової криміналістики відіграє тут не лише роль консультанта, а й процесуального гаранта надійності цифрового джерела.

У країнах з усталеною практикою використання цифрових доказів, особливу увагу приділяють також інформації з відкритих джерел, зокрема в контексті OSINT-аналітики. Така інформація розглядається як допоміжна, аналітична, здатна підтверджувати або заперечувати інші матеріали, але рідко визнається повноцінним самостійним доказом без додаткового підтвердження, експертизи або належної фіксації процесу її отримання. Міжнародна правозастосовна практика демонструє узагальнений підхід: цифровий доказ визнається допустимим лише за умови забезпечення автентичності, дотримання процесуального порядку його отримання та збереження, а також з урахуванням гарантій права на справедливий суд.

Успішна імплементація таких стандартів потребує технічної компетенції, нормативної деталізації та інституційної координації, особливо в умовах транскордонної злочинності та цифрового середовища, що постійно змінюється. Для України це означає потребу гармонізувати процесуальні правила із провідними міжнародними підходами, зокрема шляхом розробки окремого розділу КПК, присвяченого цифровим доказам, а також створення техніко-юридичних протоколів, що дозволятимуть інтегрувати результати міжнародного цифрового співробітництва у національний доказовий процес.

Висновки. У сучасному кримінальному провадженні щодо економічних злочинів цифрові докази перестали бути факультативним або другорядним елементом доказової системи. Вони дедалі частіше становлять основу обвинувачення, забезпечуючи відображення злочинної поведінки у тих цифрових слідах, які залишаються в інформаційних системах, облікових програмах, платіжних шлюзах, хмарних сервісах, криптовалютних платформах та електронному документообігу.

Їхнє значення зростає особливо в умовах транснаціонального характеру сучасної економічної злочинності, що базується на використанні складних цифрових інструментів, які нерідко приховують реальних бенефіціарів, місце вчинення правопорушення та сліди обігу активів. Попри очевидну доказову цінність, цифрові докази супроводжуються цілою низкою проблем, які виводять їх у центр науково-практичної дискусії. Основні виклики полягають у відсутності в Кримінальному процесуальному кодексі України належної дефініції цифрового доказу, нестачі процедур, що регулюють його збирання, фіксацію та збереження, а також у складності підтвердження автентичності та допустимості в умовах транснаціонального обігу інформації. Цифровий об'єкт не можна візуально оцінити, як речовий доказ; він не завжди має стабільне місце зберігання; а його зміст може бути змінено без жодного матеріального сліду, що створює серйозні виклики для судової експертизи, адвокатської перевірки та судового контролю.

Підвищення ефективності використання цифрових доказів у справах економічного спрямування потребує комплексної трансформації законодавчого, технічного та інституційного підґрунтя. Насамперед ідеться про доцільність імплементації міжнародних стандартів цифрового доказування, зокрема на базі Будапештської конвенції та протоколів e-Evidence, гармонізації національного законодавства з практикою ЄС і США щодо автентифікації та допустимості таких доказів, а також створення процесуального механізму фіксації цифрових слідів, подібного до класичного обшуку чи виїмки, але адаптованого до цифрового середовища.

Крім того, важливою умовою є підготовка фахівців з цифрової криміналістики, здатних як проводити експертизи цифрових об'єктів, так і супроводжувати процес збирання даних у спосіб, сумісний із вимогами доказового права. Особливе значення має і розвиток цифрової інфраструктури правоохоронних органів, зокрема створення цифрових лабораторій, підрозділів OSINT, а також інтеграція українських органів досудового розслідування у глобальні механізми оперативного обміну електронними доказами. Таким чином, цифрові докази стають не лише відображенням технічного прогресу в кримінальному процесі, а й маркером ефективності правоохоронної системи в її здатності адаптуватися до змін.

ЛІТЕРАТУРА:

1. Кримінальний процесуальний кодекс України: Закон України № 4651-VI від 13.04.2012 року. Електронне джерело. URL: https://zakon.rada.gov.ua/laws/show/4651-17/conv#Text

2. Авдєєва Галина, Ельжбета Живуцька-Козловська (2023) Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики* С. 126-143.

3. Фігурський В. М. (2023) Докази в електронній формі у кримінальному провадженні. *Галицькі студії: Юридичні науки* (4) С. 97-105.

4. Колодіна А. С., Т. С. Федорова Т.С. (2022) Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права* (1) С. 176-180.

5. Гуцалюк, М. В., Антонюк П. Є. (2022) Процесуальна спроможність використання електронної (цифрової) інформації як доказу в кримінальному провадженні. *Інформація і право 2* (41) С. 116-122.

6. Полотай О. І. (2023) Використання комп'ютерної криміналістики для забезпечення ефективного розслідування інцидентів інформаційної та кібербезпеки. *Вісник Львівського державного університету безпеки життєдіяльності* (28) С. 73-80.

7. Ліхтанська А. П., Михайлов В. О. (2024) Використання osint в кримінальному праві україни.» *DICTUM FACTUM 1* (15) С. 105-111.

8. Гарасимів, О., С. Марко, О. Ряшко. (2023) Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського національного університету. Серія: Право 2.75* С. 158-162.

9. Чванкін С. (2024) До питання гармонізації законодавства у сфері збирання електронних доказів та протидії кіберзлочинності. *Law. State. Technology (1)* С.52-59.

10. Ніколенко Л. М. (2024) Використання електронних доказів в кримінальному процесі зарубіжних країн. *Аналітично-порівняльне правознавство* (5) С.820-824.