DOI https://doi.org/10.30525/978-9934-26-686-7-20

ЦИФРОВІ ДОКАЗИ У ПРОТИДІЇ КІБЕРПРАВОПОРУШЕННЯМ: ПРАВОВІ, ТЕХНІЧНІ ТА ЕКСПЕРТОЛОГІЧНІ АСПЕКТИ

Гомон В. О., Мірошник Р. О., Хівренко Д. В.

ВСТУП

Динамічний розвиток інформаційних технологій та їх інтеграція у всі сфери суспільного життя зумовили появу якісно нових форм правопорушень, які потребують переосмислення установлених підходів до правозастосування. Кіберправопорушення, що охоплюють широкий спектр протиправних діянь від несанкціонованого доступу до комп'ютерних систем до складних схем легалізації злочинних доходів із використанням криптовалютних активів, становлять одну з найбільш гострих проблем сучасного правопорядку[1].

Центральним елементом будь-якого провадження, пов'язаного з кіберправопорушеннями, є цифрові докази – інформація в електронній формі, що має значення для встановлення обставин справи. Специфіка цифрових доказів полягає у їхній нематеріальній природі, легкості модифікації, потенційній масштабності обсягів даних та необхідності застосування спеціальних технічних знань для їх виявлення, фіксації та дослідження[2]. Ці характеристики створюють суттєві виклики для правової практики, оскільки традиційні процесуальні механізми не завжди адекватно враховують технічну специфіку цифрового середовища.

Стрімкий розвиток технологій блокчейну та криптовалют додає окремий вимір до цієї проблематики. Використання криптовалют у злочинній діяльності вимагає від експертного середовища володіння принципово новими інструментами – блокчейн-аналізаторами та системами на базі штучного інтелекту. Водночас результати застосування цих інструментів мають ймовірнісний характер, що потребує розробки методологічних стандартів.

Особливої актуальності набуває міжгалузевий характер проблематики цифрових доказів. Питання їх допустимості, достовірності та доказової сили виникають не лише у кримінальному провадженні, а й у цивільному та адміністративному судочинстві, господарському процесі та інших правових процедурах. Кожна з цих галузей встановлює власні вимоги до доказів та стандарти оцінки, що зумовлює необхідність формування цілісного міжгалузевого підходу до регламентації роботи з цифровими доказами.

Ця монографія присвячена комплексному дослідженню міжгалузевих викликів та перспектив, пов'язаних із кіберправопорушеннями та цифровими

[1] Конвенція про кіберзлочинність (Будапештська конвенція) від 23.11.2001. Рада Європи. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention

[2] ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization, 2012.

доказами. Метою роботи є системний аналіз правових, технічних та методологічних аспектів роботи з цифровими доказами, виявлення основних проблем їх допустимості та оцінки, а також формулювання пропозицій щодо вдосконалення нормативного регулювання та експертної практики. Особлива увага приділяється застосуванню блокчейн-аналізаторів та штучного інтелекту у криміналістичних дослідженнях криптовалют, процесуальним аспектам забезпечення цілісності цифрових доказів, а також перспективам розвитку правового регулювання у сфері протидії кіберправопорушенням.

1. Цифрові докази як міжгалузева правова категорія

1.1. Поняття та правова природа цифрових доказів

Цифровий доказ у найбільш загальному розумінні являє собою будь-яку інформацію, що зберігається або передається у цифровій формі та має доказове значення для встановлення обставин справи. Правова природа цифрових доказів характеризується низкою специфічних ознак: нематеріальністю, тобто існуванням доказової інформації у вигляді послідовності бітів, що потребує спеціальних засобів для відображення у доступній формі; легкою відтворюваністю, що породжує проблему розмежування оригіналу та копії; а також летючістю – здатністю до швидкої зміни або знищення внаслідок як цілеспрямованих дій, так і автоматичних процесів функціонування систем.

Чинне процесуальне законодавство України не містить окремого визначення цифрових доказів, натомість оперує поняттям електронних доказів. Кримінальний процесуальний кодекс розглядає електронні документи та дані в електронній формі у контексті загальної класифікації доказів. Цивільний процесуальний кодекс та Кодекс адміністративного судочинства визначають електронні докази як інформацію в електронній формі, що містить дані про обставини справи, зокрема електронні документи, вебсайти, повідомлення, метадані, бази[3] даних[4]. Таке регулювання, хоча й створює правову основу для використання цифрових доказів, залишає відкритими питання щодо процедур їх вилучення, зберігання та дослідження у справах про складні кіберправопорушення.

За джерелом походження цифрові докази охоплюють дані з комп'ютерних систем та мобільних пристроїв, мережевий трафік, журнали подій, дані з хмарних сервісів, інформацію з блокчейн-мереж, метадані файлів, а також дані з пристроїв Інтернету речей. Кожна з цих категорій має технічну специфіку, що впливає на процедури вилучення та критерії оцінки достовірності. Зокрема, дані з блокчейн-мереж мають принципову відмінність: вони є публічно-доступними, проте псевдонімними за природою, створюючи специфічні виклики для їх інтерпретації у доказуванні.

[3] Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV (зі змін.). URL: https://zakon.rada.gov.ua/laws/show/1618-15

[4] Кодекс адміністративного судочинства України : Закон України від 06.07.2005 № 2747-IV (зі змін.). URL: https://zakon.rada.gov.ua/laws/show/2747-15

1.2. Специфіка цифрових доказів у різних видах судочинства

У кримінальному процесі, де діє стандарт доказування «поза розумним сумнівом», вимоги до цифрових доказів є найсуворішими. Процедура вилучення має відповідати вимогам КПК щодо обшуку, тимчасового вилучення майна або інших слідчих дій, а порушення процедури може стати підставою для визнання доказу недопустимим. Особливого значення набуває забезпечення безперервного ланцюга зберігання цифрових доказів із документуванням кожного етапу роботи з доказом та криптографічною верифікацією цілісності даних.

У цивільному та адміністративному судочинстві стандарти допустимості є менш формалізованими, проте суди стикаються з проблемою оцінки автентичності цифрових доказів, оскільки можливість їх модифікації та фальсифікації значно вища, ніж для паперових документів. Відсутність єдиних стандартів подання цифрових доказів у цивільному процесі створює ситуацію правової невизначеності, коли прийняття або відхилення доказу значною мірою залежить від дискреції конкретного судді та його обізнаності у технічних питаннях. Особливу складність становить використання цифрових доказів у справах міжгалузевого характеру, коли одні й ті ж дані одночасно використовуються у кримінальному провадженні, цивільному позові та адміністративному провадженні, що порушує питання взаємної допустимості доказів та узгодження різних стандартів оцінки.

Забезпечення автентичності та цілісності цифрових доказів є фундаментальною передумовою їх використання у будь-якому провадженні. На відміну від матеріальних об'єктів, цифрові дані можуть бути модифіковані без залишення видимих слідів втручання, що робить питання верифікації критично важливим. Основним технічним інструментом є криптографічне хешування – обчислення унікального цифрового відбитку за допомогою алгоритмів SHA-256[5] або MD5, де будь-яка зміна у вихідних даних призводить до кардинальної зміни хеш-значення. Практична реалізація цих механізмів стикається з проблемами: хешування має відбуватися безпосередньо при вилученні, саме хеш-значення не захищає від підміни усього доказу, а зростання обсягів даних ускладнює верифікацію у справах із терабайтами інформації з множини пристроїв.

2. Кіберправопорушення та особливості їх доказування

2.1. Систематизація кіберправопорушень та збирання цифрових доказів

Кіберправопорушення поділяються на три основні групи: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних систем (несанкціонований доступ, шкідливе програмне забезпечення, DDoS-атаки); правопорушення з використанням комп'ютерних систем як засобу вчинення традиційних злочинів (шахрайство, легалізація доходів через криптовалюти, ransomware); та правопорушення, пов'язані зі змістом комп'ютерних даних.

[5] ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization, 2012.

Кожна категорія характеризується принципово відмінними механізмами вчинення, картиною слідства та вимогами до збирання доказів.

Доказування у першій групі вимагає дослідження журналів подій операційних систем та мережевого обладнання, слідів шкідливого програмного забезпечення та мережевого трафіку. Складність полягає у тому, що кваліфіковані зловмисники використовують VPN-сервіси, проксі-сервери та мережу Tor для маскування слідів. Друга група, що включає криптовалютні злочини, потребує комбінованого підходу – традиційних криміналістичних методів разом із блокчейн-аналізом та дослідженням цифрових артефактів на пристроях підозрюваних.

Фундаментальним принципом цифрової криміналістики є мінімізація впливу на досліджуваний об'єкт через створення побітових криміналістичних образів носіїв із подальшим проведенням усіх досліджень на копії. Для мобільних пристроїв використовуються спеціалізовані криміналістичні комплекси – Cellebrite (Inseyets), Oxygen Forensic Detective та інші, що забезпечують різні рівні доступу від логічного вилучення до повного фізичного образу. У контексті криптовалютних злочинів дані блокчейну є публічно доступними та не потребують спеціальних процесуальних дій для отримання, проте їх інтерпретація вимагає складних аналітичних досліджень з використанням блокчейн-аналізаторів.

Окрему проблему становить збирання летючих даних – інформації з оперативної пам'яті, що знищується при вимкненні живлення. Такі дані можуть містити сліди активних з'єднань зі зловмисниками, ключі шифрування або дані авторизації на криптовалютних сервісах. Вилучення летючих даних має здійснюватися за принципом порядку летючості, починаючи з найбільш нестабільних джерел, і потребує спеціалізованих інструментів та високої кваліфікації, оскільки будь-яка взаємодія з працюючою системою неминуче змінює її стан.

Зростаюча роль шифрування – BitLocker, LUKS, VeraCrypt, TrueCrypt, FileVault, повнодискове шифрування мобільних пристроїв – також створює суттєві перешкоди для отримання доступу до релевантних даних. Методи подолання шифрування включають пошук ключів у оперативній пам'яті або файлах гібернації, використання вразливостей конкретних реалізацій, а також залучення спеціалізованих апаратних засобів для обходу захисту. Фіксація цифрових доказів у процесуальних документах має відображати технічні параметри процедури вилучення, хеш-значення образів, серійні номери пристроїв та будь-які обставини, що можуть вплинути на цілісність даних.

3. Блокчейн-аналізатори та штучний інтелект у криміналістичних дослідженнях крипто валют

3.1. Технічні можливості блокчейн-аналізаторів та роль штучного інтелекту

Стрімке зростання використання криптовалют у злочинній діяльності, зокрема у схемах відмивання коштів, фінансування тероризму, ransomware-атаках та порушенні санкційних режимів, актуалізує питання застосування

спеціалізованих блокчейн-аналізаторів у рамках судової експертизи. Водночас виникає принципова методологічна проблема: трансформація технічної інформації з блокчейн-мереж у судовий доказ вимагає критичного переосмислення традиційних підходів до формулювання експертних висновків, оскільки результати автоматизованого аналізу часто мають ймовірнісний, а не категоричний характер.

Сучасні платформи блокчейн-аналізу – Global Ledger, Crystal Blockchain, CipherTrace, Chainalysis, Elliptic – використовують комплексний підхід до дослідження криптовалютних транзакцій: кластеризацію (поєднання адрес в один пул), графовий аналіз транзакційних ланцюгів (адреси – вузли, транзакції – зв'язки), атрибуцію гаманців до конкретних сервісів чи осіб та оцінку ризиків на основі машинного навчання. Ці системи здатні обробляти мільйони транзакцій у режимі реального часу, виявляти складні багаторівневі схеми переміщення коштів, ідентифікувати використання міксерів та встановлювати зв'язки між адресами на основі поведінкових патернів та евристичних правил.

Кожна з платформ має свої сильні сторони. Chainalysis відзначається найширшим покриттям блокчейнів та найбільшою базою атрибуційних даних, що робить її переважним інструментом для правоохоронних органів. Crystal Blockchain пропонує зручний графовий інтерфейс для візуалізації транзакційних ланцюгів. Global Ledger спеціалізується на глибокому аналізі з акцентом на точності кластеризації. Elliptic фокусується на аналізі ризиків та комплаєнсі. Обрання інструменту для експертного дослідження залежить від характеру завдання, типу блокчейну та необхідної глибини аналізу.

Штучний інтелект у блокчейн-аналізі застосовується для розв'язання декількох критичних завдань. Алгоритми машинного навчання дозволяють кластеризувати адреси одного власника навіть за відсутності явних зв'язків, базуючись на часових патернах, обсягах транзакцій та поведінкових характеристиках. Нейронні мережі розпізнають типові схеми відмивання: layering (створення множинних проміжних адрес), peel chain (створення видимості легітимної активності), використання cross-chain мостів (переміщення криптоактивів між різними блокчейнами) для ускладнення трасування. Системи на базі штучного інтелекту здійснюють автоматичну атрибуцію адрес до конкретних бірж, платіжних сервісів та міксерів на основі аналізу величезних датасетів історій транзакцій.

3.2. Виявлення схем відмивання криптовалютних активів та технічні обмеження аналізу

Легалізація злочинних доходів через криптовалюти має специфічні технічні ознаки, виявлені блокчейн-аналізом. Типові патерни включають структурування транзакцій для уникнення порогів моніторингу фінансових установ, швидке переміщення коштів між множинними адресами та блокчейнами, конвертацію у стейблкоїни, використання анонімних бірж без KYC та P2P-платформ з низькими вимогами до ідентифікації. Блокчейн-аналізатори застосовують графовий аналіз для виявлення складних транзакційних структур, характерних для layering-фази відмивання.

Однак дослідження стикається з принциповими технічними обмеженнями. Використання міксерів, де кошти множинних користувачів об'єднуються у загальний пул з подальшим розподілом на нові адреси, робить встановлення прямого зв'язку між конкретними вхідними та вихідними транзакціями математично неможливим. Privacy-орієнтовані криптовалюти – Monero з кільцевими підписами та конфіденційними транзакціями, Zcash з протоколом ZK-SNARK – унеможливлюють трасування коштів на рівні протоколу блокчейну. Децентралізовані міксери, cross-chain atomic swaps та інші технології обфускації створюють додаткові виклики для аналізу.

3.3. Ймовірнісна природа експертних висновків у блокчейн-експертизі

Принципова відмінність блокчейн-експертизи від традиційних криміналістичних досліджень полягає у ймовірнісному характері висновків, особливо коли кошти проходять через міксери або множинні етапи обфускації. Результати варіюються від високого рівня достовірності для прямих транзакцій без обфускаційних сервісів до повної неможливості встановлення зв'язку для коштів, що пройшли через міксери чи privacy-coins (Monero, Zcash, Dash). Категоричні твердження можливі лише для простих ланцюжків між ідентифікованими адресами без сервісів анонімізації.

Коли криптовалютні кошти надходять у загальний пул міксера, де змішуються з коштами інших користувачів, блокчейн-аналізатор може визначити лише ймовірнісний зв'язок між вхідними та вихідними транзакціями на основі часових збігів, статистичного аналізу обсягів та поведінкових патернів. Категорично стверджувати, що конкретні кошти, внесені певною особою, опинилися на певній вихідній адресі, технічно неможливо через архітектуру міксерів, спрямовану на розрив транзакційних зв'язків.

Використання блокчейн-аналізаторів у розслідуваннях вимагає дотримання науково обґрунтованої методології, що забезпечує відтворюваність результатів та можливість верифікації. Експерт не може обмежуватися представленням висновків програмного забезпечення як остаточних результатів дослідження. Необхідною є верифікація ключових висновків через аналіз первинних даних блокчейну з використанням альтернативних інструментів, перевірка коректності кластеризації через аналіз спільних входів транзакцій та документування всього ланцюга транзакцій з поясненням логіки встановлення зв'язків. Експертний висновок має містити інформацію про використані програмні засоби із зазначенням версій, методологію кластеризації та атрибуції, альтернативні сценарії переміщення коштів та рівень достовірності кожного встановленого зв'язку.

4. Процесуальні та методологічні аспекти роботи з цифровими доказами

4.1. Ланцюгзберігання та криптографічна верифікація цифрових доказів

Ланцюг зберігання цифрових доказів (chain of custody) являє собою безперервну документовану послідовність дій з доказом від моменту виявлення до представлення у суді. На етапі вилучення це включає фіксацію первинного стану об'єкта, реєстрацію технічних характеристик, обчислення хеш-значень та

створення криміналістичного образу з використанням апаратних блокувальників запису. Подальші етапи передбачають контрольоване зберігання в умовах, що виключають несанкціонований доступ, із документуванням кожної передачі доказу.

Криптографічне хешування є фундаментом забезпечення цілісності. Алгоритм SHA-256 вважається криптографічно стійким, тоді як MD5 має відомі вразливості до колізійних атак[6]. Практика передбачає обчислення хеш-значень на кількох рівнях – для носія загалом, окремих розділів та файлів – з використанням множинних алгоритмів одночасно. Кваліфікований електронний підпис та довірені позначки часу забезпечують додаткові гарантії цілісності та хронологічної прив'язки доказу.

У контексті блокчейн-експертизи ланцюг зберігання має особливості: дані блокчейну публічно доступні, а їх цілісність гарантована архітектурою розподіленого реєстру. Проте необхідно документувати джерела даних, конкретні вузли або API-сервіси, версії блокчейн-аналізаторів та дату аналізу, оскільки атрибуційні бази оновлюються і результати можуть дещо відрізнятися з часом.

4.2. Методологічні вимоги до експертного висновку та верифікація результатів

Експертний висновок у справах про кіберправопорушення має включати детальний опис об'єктів дослідження, перелік питань, опис методів та програмних засобів із зазначенням версій, послідовний виклад ходу дослідження та висновки з чітким зазначенням їхнього характеру – категоричного чи ймовірнісного. Особливу увагу слід приділяти обмеженням дослідження та альтернативним версіям, які не можуть бути виключені.

Для верифікації результатів автоматизованого аналізу рекомендується підхід перехресної верифікації – проведення аналізу одних і тих же даних кількома незалежними інструментами[7]. У блокчейн-аналізі це означає використання щонайменше двох платформ для кластеризації та трасування, а також перевірку висновків через ручний аналіз первинних даних за допомогою блокчейн-експлорерів. Збіг результатів, отриманих різними інструментами, суттєво підвищує достовірність висновків, тоді як розбіжності вимагають додаткового дослідження та пояснення.

Забезпечення відтворюваності вимагає фіксації версій програмного забезпечення, дати аналізу, параметрів налаштування та проміжних результатів. Водночас повна відтворюваність результатів блокчейн-аналізу може бути обмежена об'єктивними факторами – оновленням атрибуційних баз, зміною алгоритмів кластеризації та появою нових транзакцій, що змінюють контекст аналізу. Цей фактор має бути відображений у дослідницькій частині експертного висновку як об'єктивне обмеження даного виду дослідження, а не як недолік конкретної експертизи.

---

[6] MD5 Collision Demo, Peter Selinger Published Feb 22, 2006. Last updated Oct 11, 2011. URL: https://www.mscs.dal.ca/~selinger/md5collision/

[7] ISO/IEC 27042:2015. Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence. International Organization for Standardization, 2015.

5. Перспективи розвитку

Розвиток технологій підвищення конфіденційності криптовалютних транзакцій випереджає можливості аналітичних систем, що створює постійну необхідність адаптації експертних методик. Децентралізовані міксери, атомарні свопи, блокчейни з обмеженою прозорістю вимагають нових підходів до трасування коштів. Інтеграція штучного інтелекту відкриває нові можливості, проте високі показники точності на тренувальних даних не гарантують абсолютної достовірності, особливо за умови застосування контрзаходів.

Водночас застосування блокчейн-аналізаторів є абсолютно необхідним для розслідування криптовалютних злочинів, оскільки альтернативні методи фактично відсутні. Ручний аналіз мільйонів транзакцій технічно неможливий, а практика розслідування ransomware-атак та схем шахрайства демонструє, що саме ці технології забезпечили викриття злочинців. Відсутність категоричної достовірності у окремих висновках не применшує критичної важливості інструментів, а лише вимагає коректного відображення рівня достовірності.

Ключовими напрямами розвитку є формування єдиних методологічних стандартів експертиз у сфері кіберправопорушень, розробка стандартизованих шкал ймовірності для блокчейн-аналізу, підвищення кваліфікації експертів та суддів у цифрових технологіях, а також розвиток міжвідомчої взаємодії між правоохоронними органами, експертними установами та регуляторами фінансового ринку. Створення спеціалізованих підрозділів, що поєднують правову та технічну експертизу, забезпечення доступу до сучасних аналітичних інструментів та систематичне підвищення кваліфікації є необхідними умовами ефективної протидії кіберзлочинності.

Перспективними технологічними напрямами є застосування великих мовних моделей для аналізу текстових артефактів у кіберрозслідуваннях, розвиток предиктивного аналізу для прогнозування кіберзлочинів та інтеграція різнорідних джерел даних у єдині аналітичні платформи. Впровадження цих технологій у судово-експертну практику потребує ретельного наукового обґрунтування, валідації та формування чітких методологічних рамок, що забезпечують прозорість та верифікованість результатів.

ВИСНОВКИ

Цифрові докази як міжгалузева правова категорія потребують формування єдиного комплексного підходу до регламентації, що враховує технічну специфіку цифрової інформації та забезпечує баланс між ефективністю доказування й дотриманням процесуальних гарантій. Чинне законодавство, хоча й визнає електронні докази повноцінним засобом доказування, не містить достатньо детальних положень щодо процедур їх вилучення та дослідження у справах про складні кіберправопорушення. Класифікація кіберправопорушень демонструє значну різноманітність способів вчинення, що зумовлює необхідність диференційованого підходу до збирання та оцінки доказів у кожній категорії справ.

Застосування блокчейн-аналізаторів та штучного інтелекту є безальтернативним інструментом розслідування криптовалютних злочинів. Ймовірнісний характер окремих висновків не применшує їхньої доказової

цінності, а лише потребує адекватного відображення у процесуальних документах та відповідного тлумачення при судовому розгляді. Ланцюг зберігання, криптографічне хешування та інші механізми забезпечення цілісності є обов'язковими елементами роботи з цифровими доказами, без яких їх допустимість може бути поставлена під сумнів.

Актуальними завданнями залишаються розробка єдиних методологічних стандартів судової експертизи у сфері кіберправопорушень, впровадження стандартизованих шкал ймовірності для блокчейн-аналізу, підвищення кваліфікації експертів та суддів у сфері цифрових технологій, а також удосконалення нормативно-правової бази з урахуванням стрімкого технологічного розвитку. Вирішення цих завдань потребує консолідації зусиль правової науки, експертного середовища та правоохоронних органів.

АНОТАЦІЯ

Монографія присвячена комплексному дослідженню правових, технічних та методологічних аспектів використання цифрових доказів у протидії кіберправопорушенням в умовах динамічного розвитку інформаційних технологій. Авторами проаналізовано правову природу цифрових доказів як міжгалузевої категорії та виявлено системні прогалини чинного процесуального законодавства України щодо процедур їх вилучення, зберігання та дослідження у складних кіберсправах. Досліджено специфіку збирання цифрових доказів у різних видах судочинства з урахуванням відмінних стандартів допустимості та достовірності, притаманних кримінальному, цивільному й адміністративному процесам. Окрему увагу приділено застосуванню сучасних блокчейн-аналізаторів – Chainalysis, Crystal Blockchain, Global Ledger, Elliptic – та систем штучного інтелекту для виявлення схем легалізації криптовалютних активів і атрибуції транзакцій. Обґрунтовано, що результати автоматизованого блокчейн-аналізу мають ймовірнісний характер, що зумовлює необхідність розробки стандартизованих шкал достовірності та відповідного відображення рівня висновків у процесуальних документах. Розглянуто методологічні вимоги до забезпечення ланцюга зберігання цифрових доказів, криптографічної верифікації їх цілісності та відтворюваності результатів експертного дослідження. Визначено перспективні напрями розвитку судово-експертної практики, зокрема інтеграцію великих мовних моделей, предиктивного аналізу та уніфікованих аналітичних платформ у розслідування кіберзлочинів. Результати дослідження можуть бути використані для вдосконалення нормативно-правової бази, підвищення кваліфікації судових експертів і суддів, а також розбудови міжвідомчої взаємодії у сфері протидії кіберзлочинності.

Література

1. Конвенція про кіберзлочинність (Будапештська конвенція) від 23.11.2001. Рада Європи. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention

2. Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV (зі змін.). URL: https://zakon.rada.gov.ua/laws/show/1618-15

3. Кодекс адміністративного судочинства України : Закон України від 06.07.2005 № 2747-IV (зі змін.). URL: https://zakon.rada.gov.ua/laws/show/2747-15

4. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization, 2012.

5. NIST Special Publication 800-86. Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology. Gaithersburg, 2006. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

6. MD5 Collision Demo, Peter Selinger Published Feb 22, 2006. Last updated Oct 11, 2011. URL: https://www.mscs.dal.ca/~selinger/md5collision/

7. ISO/IEC 27042:2015. Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence. International Organization for Standardization, 2015.

Information about the authors:
Homon Volodymyr Oleksiyovych,
Forensic expert (digital evidence)
Scientific research center for forensic science of information technologies and intellectual property
26, L. Ukrainky blvd, Kyiv, 01133, Ukraine
https://orcid.org/0000-0001-6326-9590

Miroshnyk Ruslan Oleksandrovych,
Forensic expert (digital evidence)
Scientific research center for forensic science of information technologies and intellectual property,
26, L. Ukrainky blvd, Kyiv, 01133, Ukraine
https://orcid.org/0009-0004-8504-0489

Khivrenko Dmytro Volodymyrovych,
Forensic expert (digital evidence)
Scientific research center for forensic science of information technologies and intellectual property,
26, L. Ukrainky blvd, Kyiv, 01133, Ukraine