УДК 343.985:343.72:004
DOI https://doi.org/10.32782/cuj-2026-2-9

Груздь Олександр Іванович
кандидат юридичних наук,
завідувач кафедри кримінального процесу та криміналістики
факультету підготовки фахівців для органів досудового розслідування
Національної поліції України
Донецького державного університету внутрішніх справ
ORCID: 0000-0003-0370-3791

Ягольник Олег Михайлович
викладач кафедри кримінального процесу та криміналістики
факультету підготовки фахівців для органів досудового розслідування
Національної поліції України
Донецького державного університету внутрішніх справ
ORCID: 0009-0008-2867-4273

ІННОВАЦІЙНІ МЕТОДИ ІДЕНТИФІКАЦІЇ ТА ДОКУМЕНТУВАННЯ ДІЯЛЬНОСТІ ОРГАНІЗОВАНИХ КІБЕРЗЛОЧИННИХ УГРУПОВАНЬ

Інноваційні методи ідентифікації та документування діяльності організованих кіберзлочинних угруповань. У статті досліджено комплекс інноваційних методів ідентифікації учасників організованих кіберзлочинних угруповань та документування їх протиправної діяльності в контексті кримінального провадження. Встановлено, що ефективна ідентифікація в сучасних умовах базується на принципі мультиджерельної кореляції цифрових даних, оскільки жоден окремий технічний показник не є достатнім для доведення причетності особи до вчинення кримінального правопорушення. Проаналізовано метод глибокого аналізу мережевих артефактів (network artifact correlation), який передбачає комплексне дослідження технічних параметрів мережевого з'єднання – значень TTL (Time To Live – час життя пакета), TCP Window Size, наборів TCP-опцій та часових інтервалів між пакетами, – що формують «мережевий відбиток» пристрою навіть за умов використання VPN (Virtual Private Network – віртуальна приватна мережа) або TOR-інфраструктури (The Onion Router). Висвітлено метод TLS/SSL-фінгерпринтингу (Transport Layer Security / Secure Sockets Layer) за алгоритмами JA3/JA4, блокчейн-кластеризацію з використанням multi-input heuristic, OSINT-кореляцію (Open Source Intelligence – розвідка на основі відкритих джерел) псевдонімів, лінгвістичну атрибуцію (stylometric profiling), аналіз схожості шкідливого коду (code similarity detection), поведінкову біометрію та метод цифрового пристроєвого відбитка. Окрему увагу приділено процедурам криміналістичного документування електронних доказів: застосуванню write-blocker-пристроїв, bit-by-bit копіюванню, обчисленню криптографічних хеш-сум (MD5, SHA-256) та забезпеченню безперервності ланцюга зберігання доказів (chain of custody). Обґрунтовано, що комплексне застосування описаних методів формує багаторівневу модель атрибуції, яка поєднує технічні, фінансові та поведінкові маркери і відповідає вимогам допустимості та достовірності електронних доказів у кримінальному процесі. Зроблено висновок про необхідність систематичного впровадження інтегрованих аналітичних платформ, підвищення кваліфікації слідчих у сфері цифрової криміналістики та посилення міжнародної правової співпраці у сфері протидії кіберзлочинності.

Ключові слова: *кіберзлочинне угруповання, кримінальне правопорушення, цифровий доказ, мережева атрибуція, криміналістичне документування, блокчейн-кластеризація, code similarity detection, ланцюг зберігання доказів.*

Hruzd O. I., Yagolnik O. M. Innovative methods of identification and documentation of organized cybercriminal groups' activities

Innovative methods of identification and documentation of organized cybercriminal groups' activities. The article examines a comprehensive set of innovative methods for identifying members of organized cybercriminal groups and documenting their unlawful activities in the context of criminal proceedings. It is established that effective identification under modern conditions is based on the principle of multi-source digital data correlation, since no single technical indicator is sufficient to prove a person's involvement in a criminal offense. The method of deep network artifact correlation is analyzed, comprising complex examination of technical parameters of network connections – TTL (Time To Live) values, TCP Window Size, TCP option sets, and inter-packet timing – which form the "network fingerprint" of a device even when VPN (Virtual Private Network) or TOR (The Onion Router) infrastructure is used. The article also addresses TLS/SSL (Transport Layer Security / Secure Sockets Layer) fingerprinting via JA3/JA4 algorithms, blockchain clustering using multi-input heuristics, OSINT (Open Source Intelligence) correlation of pseudonyms, linguistic attribution (stylometric profiling), malicious code similarity detection, behavioral biometrics, and digital device fingerprinting. Special attention is given to forensic documentation procedures for electronic evidence: the use of write-blocker devices, bit-by-bit imaging, computation of cryptographic hash values (MD5, SHA-256), and maintaining the chain of custody. It is argued that the integrated application of these methods creates a multi-layered attribution model combining technical, financial, and behavioral markers that satisfies the requirements of admissibility and reliability of electronic evidence in criminal proceedings. The conclusion is drawn regarding the necessity of systematic implementation of integrated analytical platforms, enhanced training of investigators in digital forensics, and strengthened international legal cooperation in combating cybercrime.

Key words: *cybercriminal group, criminal offense, digital evidence, network attribution, forensic documentation, blockchain clustering, code similarity detection, chain of custody.*

Вступ. Стрімкий розвиток цифрових технологій зумовив не лише якісну зміну форм злочинної діяльності, але й суттєво ускладнив її виявлення та доказування. Організовані кіберзлочинні угруповання, що здійснюють кримінальні правопорушення у сфері використання комп'ютерів, комп'ютерних мереж та телекомунікаційних систем, широко застосовують інструменти анонімізації: VPN-сервіси (Virtual Private Network – віртуальні приватні мережі), мережу TOR (The Onion Router), проксі-інфраструктуру та криптовалютні розрахунки. Це суттєво обмежує ефективність традиційних криміналістичних методів і вимагає впровадження принципово нових підходів до ідентифікації учасників угруповань і документування їхньої діяльності. Особливої актуальності це питання набуває в контексті забезпечення допустимості та достовірності електронних доказів у кримінальному провадженні, оскільки формальні процедурні порушення при зборі цифрових слідів можуть призвести до їх недопустимості навіть за умови технічно бездоганної атрибуції. Таким чином, розробка теоретичної основи і практичних рекомендацій щодо застосування інноваційних методів ідентифікації та документування кіберзлочинних угруповань є нагальною науковою та практичною потребою.

Матеріали та методи. Методологічну основу дослідження становлять загальнонауковий діалектичний метод, системний підхід до аналізу цифрових засобів атрибуції та криміналістичного документування, а також порівняльний аналіз вітчизняної та зарубіжної практики кіберрозслідувань. При дослідженні методів ідентифікації застосовувався аналітико-синтетичний метод, а при розгляді процедур документування – формально-юридичний метод для забезпечення відповідності пропонованих рекомендацій вимогам КПК України (Кримінального процесуального кодексу України). Інформаційною базою дослідження слугували наукові праці у сфері кіберкриміналістики та кримінально-правової протидії кіберзлочинності [1–10], стандарти цифрової форензіки NIST SP 800-101r1 [11], ISO/IEC 27037:2012 [12], рекомендації ENISA (Агентства Європейського Союзу з кібербезпеки) [13], а також практика розслідування кримінальних правопорушень у сфері інформаційних технологій.

Результати. Ефективна ідентифікація організованих кіберзлочинних угруповань сьогодні базується на принципі мультиджерельної кореляції даних. Жоден окремий технічний показник не є достатнім для доведення причетності

особи до вчинення кримінального правопорушення, тому застосовується поєднання мережевої, фінансової, поведінкової та лінгвістичної аналітики. Практика кіберрозслідувань демонструє, що результат досягається саме через накладання кількох незалежних цифрових маркерів. Такий підхід дозволяє компенсувати використання правопорушниками VPN, TOR та проксі-інфраструктури. Саме комплексність стає ключовою умовою достовірної атрибуції.

Як вказує В. Шакун, одним із базових практичних методів ідентифікації учасників організованих кіберзлочинних угруповань є глибокий аналіз мережевих артефактів. Йдеться не лише про встановлення IP-адреси джерела трафіку, а про комплексне дослідження технічних характеристик мережевого з'єднання, які формують «мережевий відбиток» пристрою. Під час реагування на інцидент фіксуються первинні пакети з'єднання, зберігаються PCAP-файли (Packet Capture – файли захоплення мережевих пакетів) та здійснюється їх подальший технічний розбір [1, с. 80]. Досліджуються такі параметри: значення TTL (Time To Live – час життя пакета), що може вказувати на тип операційної системи; розмір TCP Window Size та його варіації; набір TCP-опцій (зокрема MSS – Maximum Segment Size, SACK – Selective Acknowledgment, Timestamp); особливості формування SYN-пакетів; часові інтервали між пакетами (packet timing patterns). Сукупність цих характеристик дозволяє сформувати профіль конкретної мережевої конфігурації. Навіть при зміні IP через VPN або проксі більшість параметрів залишаються незмінними і використовуються як додаткові маркери ідентифікації.

На думку С. Чванкіна, практичне значення має також аналіз поведінки TCP/IP-стеку операційної системи. Різні версії Windows, Linux або macOS мають характерні особливості формування мережевих пакетів. За допомогою інструменту p0f (passive OS fingerprinter – пасивний інструмент визначення операційної системи) можливо здійснити пасивне визначення ОС без активного втручання. Якщо однаковий профіль фіксується в кількох інцидентах, це може свідчити про використання одного й того самого пристрою або віртуального середовища – у сукупності з іншими даними це суттєво підсилює доказову базу у кримінальному провадженні [2, с. 58].

Реальним інструментом ідентифікації є TLS/SSL-фінгерпринтинг за алгоритмами JA3 та JA4 (методи хешування параметрів TLS-з'єднання, розроблені компанією Salesforce). Кожен клієнт формує унікальний набір параметрів шифрування під час встановлення захищеного з'єднання. Хешування цих параметрів дозволяє створити цифровий відбиток конкретного програмного середовища. Якщо однаковий JA3-фінгерпринт з'являється у різних інцидентах, це вказує на використання одного інструменту або конфігурації – метод широко застосовується в аналітичних центрах кібербезпеки.

Практично значущим є аналіз повторного використання інфраструктури (infrastructure reuse analysis). Кіберугруповання часто використовують однакові шаблони реєстрації доменів, DNS-сервери (Domain Name System – система доменних імен) або специфічні SSL-сертифікати. Через сервіси Censys, Shodan та PassiveTotal можна відстежити історію змін доменних записів, а повторюваність контактних email або технічних параметрів реєстрації дозволяє об'єднати атаки в одну кампанію [3, с. 79].

Одним із найбільш результативних сучасних методів є блокчейн-кластеризація. Застосовується multi-input heuristic (евристика спільного введення), що дозволяє об'єднувати адреси в один контрольований кластер, а аналіз change-адрес визначає гаманці, які повертають залишки коштів. Подальша ідентифікація здійснюється через точки входу в регульовані біржі з процедурами KYC (Know Your Customer – принцип «знай свого клієнта») – це формує фінансову модель діяльності угруповання і є одним із найбільш переконливих доказових інструментів у справах щодо кримінальних правопорушень із використанням криптовалюти.

У практиці документування важливу роль відіграє OSINT-кореляція псевдонімів (Open Source Intelligence – розвідка на основі відкритих джерел): аналізується повторне використання nickname у різних форумах,

GitHub-репозиторіях та месенджерах. Навіть незначні варіації написання можуть вказувати на одну особу. Інструменти типу Maltego або SpiderFoot дозволяють автоматизувати цей процес – повторюваність цифрової ідентичності часто стає ключем до деанонімізації.

Лінгвістична атрибуція (stylometric profiling – стилометричне профілювання) використовується для встановлення автора текстових повідомлень або шкідливого коду. Аналізується структура речень, частота функціональних слів, специфічні орфографічні помилки. Алгоритми машинного навчання дозволяють визначити ймовірність авторства з високою точністю, причому лінгвістичні патерни складно повністю змінити навіть свідомо [4, с. 175]. Цей метод особливо ефективний щодо адміністраторів даркнет-форумів. Разом з тим слід зауважити, що його застосування потребує додаткового обґрунтування допустимості в суді, адже у вітчизняній судовій практиці відсутні усталені стандарти оцінки стилометричних висновків.

Аналіз часових патернів активності (timestamp analysis) передбачає фіксацію часу входів у панелі керування, моментів запуску атак і публікацій у чатах. Порівняння цих даних дозволяє визначити часову зону оператора. Якщо активність систематично припиняється у певні години, це вказує на регіон перебування. Поєднання з мовною атрибуцією значно звужує коло підозрюваних у кримінальному провадженні.

Ефективним методом технічної атрибуції є аналіз схожості шкідливого коду (code similarity detection), який дозволяє встановити зв'язок між різними зразками malware (шкідливого програмного забезпечення). На відміну від сигнатурного антивірусного підходу, цей метод спрямований на виявлення спільної логіки, архітектури та стилю програмування. Навіть якщо правопорушник змінює назви файлів, шифрує рядки або застосовує пакування, базові алгоритмічні конструкції часто залишаються подібними й стають об'єктом порівняльного аналізу [4, с. 176].

На практиці використовується як статичний аналіз (дослідження дизасембльованого або декомпільованого коду через IDA Pro, Ghidra, Radare2), так і динамічний аналіз у sandbox-середовищі (Cuckoo Sandbox, Any.Run), де фіксується поведінка програми під час виконання. Досліджуються: структура основних функцій і модулів; реалізація алгоритмів шифрування; послідовність викликів Windows API (Application Programming Interface – інтерфейс програмування застосунків); використання однакових бібліотек; характерні помилки або коментарі розробника. Повторюваність цих ознак у різних зразках свідчить про спільне джерело походження [5, с. 281].

Додатково застосовуються алгоритми fuzzy hashing (нечіткого хешування) – ssdeep та TLSH, – які визначають ступінь подібності файлів навіть при часткових змінах структури. Це дозволяє відстежити еволюцію шкідливого ПЗ у межах однієї злочинної кампанії і довести належність кількох атак до одного угруповання [6, с. 445]. Такий підхід є особливо результативним при розслідуванні ransomware-кампаній (від англ. ransom – викуп), де різні «збірки» шифрувальника розповсюджуються різними афілійованими особами. Водночас необхідно враховувати правові обмеження використання таких методів: у деяких юрисдикціях для отримання зразків шкідливого ПЗ від третіх сторін може вимагатися судовий дозвіл [14].

Перспективним методом є поведінкова біометрія: аналізується ритм набору тексту, швидкість реакції та патерни руху миші. Навіть при використанні іншого акаунта поведінкові характеристики залишаються подібними. Цей метод застосовується банківськими установами й може використовуватися як додатковий доказ у кримінальному провадженні, доповнюючи технічну атрибуцію. Слід, однак, зазначити, що в умовах використання правопорушниками засобів автоматизації (ботів) ефективність методу може суттєво знижуватися.

Метод кореляції витоків даних (leak intelligence analysis) передбачає пошук email або паролів, що з'являються у кількох злитих базах, що формує ланцюг зв'язків і нерідко дозволяє встановити реальну особу за псевдонімом. Практика показує, що недбалість у цифровій гігієні є поширеною серед осіб, причетних до кримінальних правопорушень у кіберпросторі [10, с. 67].

Важливу роль відіграє також створення контрольованих honeypot-середовищ (від англ. honey pot – горщик меду; приманка для зловмисників), що дозволяють зафіксувати повну послідовність команд правопорушника. Командна історія містить характерні скорочення, синтаксис та помилки; іноді оператори випадково залишають тестові IP або внутрішні домени, які стають критичними для ідентифікації. Разом з тим застосування honeypot-методів має відповідати принципу законності: у деяких країнах провокування злочинної діяльності через такі середовища може вважатися агентурною провокацією і призводити до недопустимості зібраних доказів. Метод цифрового пристроєвого відбитка (device fingerprinting) доповнює цей арсенал, збираючи дані про конфігурацію браузера, шрифти, роздільну здатність екрану, що формує практично унікальний профіль, сталий навіть при зміненому IP [7, с. 183].

У документуванні діяльності організованих кіберзлочинних угруповань ключовим є правильне створення форензічних копій цифрових носіїв із використанням апаратних або програмних write-blocker-пристроїв (пристроїв захисту від запису). Write-blocker унеможливлює будь-який запис на оригінальний носій, гарантуючи збереження його первинного стану – вимога, закріплена стандартом ISO/IEC 27037:2012 [12]. Перед початком копіювання фіксуються тип носія, серійний номер, фізичний стан та умови вилучення. Сам процес здійснюється спеціалізованими інструментами (FTK Imager, EnCase, X-Ways Forensics) із формуванням повного bit-by-bit копіювання (побітового копіювання) – це дозволяє зберегти не лише активні файли, але й видалені дані та службові області диска.

Обов'язковим елементом процедури є обчислення криптографічних хеш-сум (MD5 – Message Digest Algorithm 5, SHA-1 та SHA-256 – Secure Hash Algorithm) до початку копіювання та після його завершення. Співпадіння значень підтверджує цілісність створеної копії та відсутність змін у процесі роботи. Хеш-значення заносяться до протоколу слідчої дії та зберігаються разом із матеріалами провадження. У разі передачі носія або копії іншому експерту здійснюється повторна перевірка контрольних сум – це забезпечує безперервність ланцюга зберігання доказів (chain of custody) [8, с. 144].

Протоколи документування детально фіксують: дату, час і місце вилучення носія; посаду та дані особи, яка здійснювала копіювання; технічні характеристики обладнання; назву та версію програмного забезпечення; алгоритм хешування. Судова практика демонструє, що саме формальна коректність документування нерідко визначає допустимість електронного доказу [9, с. 37]. Будь-які подальші дослідження здійснюються виключно з форензічної копії, а оригінальний носій зберігається у спеціальних умовах із обмеженим доступом. При роботі з мобільними пристроями застосовуються режими ізоляції від мережі (Faraday bags – клітки Фарадея) для запобігання дистанційному видаленню даних.

Додаткової достовірності доказам надають централізована кореляція логів через SIEM-платформи (Security Information and Event Management – системи управління інформацією та подіями безпеки), що автоматично пов'язують події з різних систем і формують єдину шкалу часу інциденту, та timestamp-верифікація із застосуванням кваліфікованих електронних міток часу або блокчейн-фіксації хешів, що виключає можливість подальшої зміни доказів без сліду.

Висновки. Проведене дослідження засвідчує, що ефективна протидія організованим кіберзлочинним угрупованням, які вчиняють кримінальні правопорушення у сфері інформаційних технологій, неможлива без впровадження комплексних інноваційних методів ідентифікації та документування їх діяльності. Традиційні підходи, засновані виключно на встановленні IP-адрес чи вилученні окремих носіїв інформації, не відповідають сучасним умовам анонімізації та розподіленої злочинної інфраструктури.

Найбільш результативною є модель мультифакторної атрибуції, яка поєднує мережевий аналіз (network artifact correlation, TLS-фінгерпринтинг), блокчейн-кластеризацію, OSINT-кореляцію псевдонімів, лінгвістичну атрибуцію (stylometric profiling), аналіз схожості коду (code similarity detection),

поведінкову біометрію та кореляцію витоків даних. Інтеграція різних цифрових маркерів дозволяє формувати належну та допустиму доказову базу у кримінальному провадженні.

Встановлено, що особливого значення набуває належне процесуальне документування електронних доказів із дотриманням принципу безперервності ланцюга їх зберігання (chain of custody). Використання форензічних копій, хеш-контролю, цифрових міток часу та стандартизованої звітності забезпечує збереження цілісності доказової інформації відповідно до вимог кримінального процесуального законодавства та міжнародних стандартів (NIST SP 800-101r1, ISO/IEC 27037:2012).

Перспективним напрямом подальшого розвитку є створення інтегрованих аналітичних платформ, що забезпечують автоматизовану кореляцію даних з різних джерел, підвищення кваліфікації фахівців у сфері цифрової криміналістики та посилення міжнародної правової допомоги щодо отримання технічних даних від VPN-провайдерів і хостинг-платформ. Системний характер застосування описаних методів сприятиме підвищенню рівня розкриття кримінальних правопорушень у сфері кіберзлочинності та зміцненню інформаційної безпеки держави.

Література

1. Шакун В.І. Аналіз злочинності: проблеми термінології. Філософські та методологічні проблеми права. 2023. № 2 (26). С. 73–81. DOI: https://doi.org/10.33270/02232602.73

2. Чванкін С. До питання гармонізації законодавства у сфері збирання електронних доказів та протидії кіберзлочинності. *Law. State. Technology*. 2024. Вип. 1. С. 52–59. DOI: https://doi.org/10.32782/LST/2024-1-8

3. Полотай О.І. Використання комп'ютерної криміналістики для забезпечення ефективного розслідування інцидентів інформаційної та кібербезпеки. *Вісник Львівського державного університету безпеки життєдіяльності.* 2023. №28. С. 73–80. DOI: https://doi.org/10.32447/20784643.28.2023.07

4. Гуцалюк М.В. Стратегії протидії сучасним кіберзагрозам та забезпечення кіберстійкості критичної інфраструктури України. *Інформація і право.* 2024. № 2(49). С. 164–177. DOI: https://doi.org/10.37750/2616-6798.2024.2(49).306199

5. Попко В.В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі. *Науковий вісник Ужгородського національного університету.* 2021. № 66. С. 276–283. DOI: https://doi.org/10.24144/2307-3322.2021.66.46

6. Бодунова О.М. Історико-правові аспекти виникнення злочинності у сфері інформаційних технологій. *Аналітично-порівняльне правознавство*. 2023. № 1. С. 441–445. DOI https://doi.org/10.24144/2788-6018.2023.01.76

7. Воронов І.О. Криміналістичний аналіз кримінальних правопорушень у сфері використання комп'ютерів. *Юридичний бюлетень*. 2022. Вип. 24. С. 180–186.

8. Довженко О.Ю. До питання про тактику допитів у справах про кіберзлочини. *Науковий вісник Міжнародного гуманітарного університету*. 2019. № 37. С. 143–145.

9. Кіберзлочинність та електронні докази / Б. М. Головкін та ін.; за ред. О. Денькович, Г. Шмельцер. Львів: ЛНУ ім. Івана Франка, 2022. 298 с.

10. Діордіца І.В. Кримінально-правова сутність кібершпигунства. Реалії та перспективи розбудови правової держави в Україні та світі: матеріали III міжнар. наук.-практ. конф., м. Суми, 2020. С. 66–69.

11. NIST Special Publication 800-101 Revision 1: Guidelines on Mobile Device Forensics / National Institute of Standards and Technology. Gaithersburg, 2014. 87 p. DOI: https://doi.org/10.6028/NIST.SP.800-101r1

12. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012. 36 p.

13. ENISA. Electronic evidence – a basic guide for First Responders. Good practice material for CERT first responders. European Union Agency for Cybersecurity. Luxembourg: Publications Office of the EU, 2014. 57 p. URL: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders (дата звернення 15.03.2026)

14. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. Amsterdam: Academic Press, 2011. 838 p.

References

1. Shakun, V.I. (2023). Analiz zlochynnosti: problemy terminolohii [Analysis of crime: problems of terminology]. *Filosofski ta metodolohichni problemy prava.* № 2 (26). S. 73–81. DOI: https://doi.org/10.33270/02232602.73 [in Ukrainian]

2. Chvankin, S. (2024). Do pytannia harmonizatsii zakonodavstva u sferi zbyrannia elektronnykh dokaziv ta protydii kiberzlochynnosti [On the harmonization of legislation in the field of electronic evidence collection and combating cybercrime]. *Law. State. Technology*. (1). S. 52–59. DOI: https://doi.org/10.32782/LST/2024-1-8 [in Ukrainian]

3. Polotai, O.I. (2023). Vykorystannia kompiuternoi kryminalistyky dlia zabezpechennia efektyvnoho rozsliduvannia intsydentiv informatsiinoi ta kiberbezpeky [Use of computer forensics for effective investigation of information and cybersecurity incidents]. *Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti*. (28). S. 73–80. DOI: https://doi.org/10.32447/20784643.28.2023.07 [in Ukrainian]

4. Hutsaliuk, M.V. (2024). Stratehii protydii suchasnym kiberzahrozam ta zabezpechennia kiberstiikosti krytychnoi infrastruktury Ukrainy [Strategies for countering modern cyber threats and ensuring cyber resilience of Ukraine's critical infrastructure]. *Informatsiia i pravo*. № 2(49). S. 164–177. DOI: https://doi.org/10.37750/2616-6798.2024.2(49).306199 [in Ukrainian]

5. Popko, V.V. (2021). Mizhnarodno-pravova rehlamentatsiia transnatsionalnoi kiberzlochynnosti u kiberprostori [International legal regulation of transnational cybercrime in cyberspace]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu*. № 66. S. 276–283. DOI: https://doi.org/10.24144/2307-3322.2021.66.46 [in Ukrainian]

6. Bodunova, O.M. (2023). Istoryko-pravovi aspekty vynyknennia zlochynnosti u sferi informatsiinykh tekhnolohii [Historical and legal aspects of the emergence of crime in the field of information technologies]. *Analitychno-porivnialne pravoznavstvo.* № 1. S. 441–445. DOI https://doi.org/10.24144/2788-6018.2023.01.76 [in Ukrainian]

7. Voronov, I.O. (2022). Kryminalistychnyi analiz kryminalnykh pravoporushen u sferi vykorystannia kompiuteriv [Forensic analysis of criminal offenses in the field of computer use]. *Yurydychnyi biuleten.* № 24. S. 180–186. [in Ukrainian]

8. Dovzhenko, O.Yu. (2019). Do pytannia pro taktyku dopytiv u spravakh pro kiberzlochyny [On the tactics of interrogations in cybercrime cases]. Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. № 37. S. 143–145. [in Ukrainian]

9. Kiberzlochynnist ta elektronni dokazy [Cybercrime and digital evidence] / Holovkin, B.M. ta in.; za red. O. Denkovych, H. Shmeltsera. (2022). Lviv: LNU im. Ivana Franka. [in Ukrainian]

10. Diorditsia, I.V. (2020). Kryminalno-pravova sutnist kibershpyhunstva [The criminal law essence of cyberespionage]. *Realii ta perspektyvy rozbudovy pravovoi derzhavy v Ukraini ta sviti*: materialy III mizhnar. nauk.-prakt. konf., m. Sumy. S. 66–69. [in Ukrainian]

11. National Institute of Standards and Technology (2014). NIST Special Publication 800-101 Revision 1: Guidelines on Mobile Device Forensics. Gaithersburg: NIST. URL: https://doi.org/10.6028/NIST.SP.800-101r1.

12. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. (2012). Geneva: ISO.

13. ENISA (2014). Electronic evidence – a basic guide for First Responders. Luxembourg: Publications Office of the EU. URL: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders.

14. Casey E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed. Amsterdam: Academic Press.

Дата першого надходження статті до видання: 10.04.2026
Дата прийняття статті до друку після рецензування: 11.05.2026
Дата публікації (оприлюднення) статті: 29.05.2026