УДК 343.346.8:004
DOI https://doi.org/10.24144/2307-3322.2025.92.4.55

РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ: СУЧАСНІ ВИКЛИКИ ТА КРИМІНАЛІСТИЧНІ ОСОБЛИВОСТІ

Попович М.В.,
доктор філософії (PhD),
асистент кафедри кримінального права
юридичного факультету,
Чернівецький національний університет ім. Юрія Федьковича
ORCID: 0000-0003-4807-6621

Продан Т.В.,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права,
Чернівецький національний університет ім. Юрія Федьковича
ORCID: 0000-0001-6347-0606

Попович М.В., Продан Т.В. Розслідування кіберзлочинів: сучасні виклики та криміналістичні особливості.

У статті проаналізовано особливості розслідування кіберзлочинів. Зростаюча цифровізація критичної інфраструктури посилила загрозу кіберзлочинності в усіх установах, що працюють з високовартісними активами та конфіденційною інформацією. Це дослідження заповнює прогалину, оцінюючи реальну ефективність комп'ютерно-криміналістичних методів для виявлення та розслідування злочинів у великих галузях, включно з фінансами, роздрібною торгівлею та технологіями. Досліджується використання криміналістичних інструментів для виявлення доказів у складних кримінальних провадженнях, причому найефективнішими виявилися відновлення даних та статистичний аналіз. На відміну від подібних досліджень, ця робота інтегрує емпіричні дані та експертні оцінки для аналізу реальних викликів і внеску цифрової криміналістики на практиці, наголошується на необхідності проведення додаткового навчання працівників правоохоронної системи, які безпосередньо проводять досудове розслідування даної категорії справ. Дослідження робить внесок у літературу, розробляючи секторальну криміналістичну рамку, визначаючи правові та процедурні обмеження та пропонуючи шляхи впровадження інструментів штучного інтелекту в криміналістичну діяльність. Окрім аналізу сучасних методів цифрової криміналістики, у статті розглянуто перспективи розвитку інноваційних технологій у сфері розслідування кіберзлочинів. Особливу увагу приділено застосуванню алгоритмів машинного навчання для автоматизації процесів виявлення аномалій та прогнозування потенційних загроз. Акцентовано увагу на необхідність гармонізації національного законодавства з міжнародними стандартами, що дозволить ефективніше координувати діяльність правоохоронних органів різних країн. Отримані результати мають практичне значення для підвищення точності розслідувань, оптимізації розподілу ресурсів та міжвідомчої співпраці у сфері протидії та розслідування кіберзлочинності.

Ключові слова: досудове розслідування, комп'ютерна криміналістика, безпека критичної інфраструктури, аналіз цифрових доказів, кіберзлочинність, методи криміналістичних розслідувань, штучний інтелект у цифровій криміналістиці.

Popovich M.V., Prodan T.V. Investigation of cybercrimes: current challenges and forensic features.

The article analyzes the peculiarities of cybercrime investigation. The growing digitization of critical infrastructure has increased the threat of cybercrime in all institutions that work with high-value assets and confidential information. This study fills a gap by assessing the real effectiveness of computer

forensics methods for detecting and investigating crimes in major industries, including finance, retail, and technology. It examines the use of forensic tools to uncover evidence in complex criminal proceedings, with data recovery and statistical analysis proving to be the most effective. Unlike similar studies, this work integrates empirical data and expert assessments to analyze the real challenges and contributions of digital forensics in practice, emphasizing the need for additional training for law enforcement personnel who directly conduct pre-trial investigations of this category of cases. The study contributes to the literature by developing a sectoral forensic framework, identifying legal and procedural constraints, and proposing ways to implement artificial intelligence tools in forensic activities. In addition to analyzing modern methods of digital forensics, the article discusses the prospects for the development of innovative technologies in the field of cybercrime investigation. Particular attention is paid to the use of machine learning algorithms to automate the processes of detecting anomalies and predicting potential threats. Emphasis is placed on the need to harmonize national legislation with international standards, which will allow for more effective coordination of the activities of law enforcement agencies in different countries. The results obtained are of practical importance for improving the accuracy of investigations, optimizing the allocation of resources, and interagency cooperation in the field of countering and investigating cybercrime.

Key words: pre-trial investigation, computer forensics, critical infrastructure security, digital evidence analysis, cybercrime, forensic investigation methods, artificial intelligence in digital forensics.

Постановка проблеми. В епоху всеосяжної цифровізації критичні інфраструктурні комплекси – фінансові, комерційні чи технологічні – дедалі більше залежать від складних інформаційних технологій. Разом із цим прогресом зростає й операційна ефективність, але водночас і вразливість до небачених раніше кібернападів. Злочини проти таких інфраструктур, особливо підприємницької діяльності, становлять реальну загрозу економічній стабільності, національній безпеці та громадській безпеці. Такі злочини часто супроводжуються складними кіберзлочинними змовами, включно з витоками даних, розкраданням коштів, фінансовим шахрайством та несанкціонованими вторгненнями в комп'ютерні системи, що потребують застосування передових технічних методів ідентифікації та розслідування.

Мета дослідження полягає у виробленні науково обґрунтованих рекомендацій щодо оптимізації цифрових криміналістичних методів у боротьбі з кіберзлочинністю, з урахуванням процедурних та правових викликів, а також можливостей застосування штучного інтелекту для підвищення точності та ефективності розслідувань. Формування комплексного підходу до оцінки та вдосконалення комп'ютерної криміналістики у сфері кіберзлочинів, що включає аналіз сучасних методів, правових та процедурних аспектів.

Стан опрацювання проблематики. Хоча цифрова криміналістика стала цінним інструментом у розслідуванні кіберзлочинів, наявна література здебільшого розглядає загальні кіберінциденти. Серед науковців даним питанням займалися: Колодіна А.С., Федорова Т.С., Гори І.В., Колесник В.А., Попович І.І. та інші.

Варто розпочати з імперичних досліджень, які у великому масштабі, що оцінюють ефективність криміналістичних методів у різних галузях та юрисдикціях, є рідкісними. Криміналістичне дослідження злочинів також ускладнюється правовою невизначеністю щодо допустимості, обробки та процедурного використання цифрових доказів. Внутрішня складність корпоративних комп'ютерних систем, поєднана з індивідуально розробленими технологіями та функціонуванням у різних регуляторних режимах, вимагає адаптованого криміналістичного підходу. Це дослідження заповнює прогалину шляхом систематичної оцінки ефективності комп'ютерно-криміналістичних методів у кримінальних розслідуваннях злочинів у підприємницькій діяльності об'єктів критичної інфраструктури, тощо.

Виклад основного матеріалу. Варто зазначити, що науковці А.С. Колодіна, Т.С. Федорова у статті «Цифрова криміналістика: проблеми теорії і практики» підкреслюють, що сучасні інформаційні технології вивели криміналістичну експертизу на новий етап розвитку. Автори наголошують на важливості методів пошуку, отримання та закріплення цифрових доказів, які часто є «невидимими» у традиційних слідчих процедурах. Автори підкреслюють, що сучасні інформаційні технології радикально змінили підхід до криміналістичної експертизи. Якщо раніше акцент робився на матеріальних доказах (сліди, документи, речові докази), то тепер ключову роль відіграють цифрові артефакти. Також автори акцентують увагу на «Невидимі докази»: йдеться про

дані, які не можна побачити без спеціальних інструментів – метадані, приховані файли, системні журнали, залишкові сліди у пам'яті пристроїв. Вони часто залишаються поза увагою традиційних слідчих процедур. Автори наголошують на важливості використання спеціалізованого програмного забезпечення для вилучення та збереження цифрових доказів у незмінному вигляді, щоб гарантувати їхню допустимість у суді. Звертається увага на недоліки в українському законодавстві адже досі бракує чітких норм щодо допустимості цифрових доказів, виникають труднощі з їхньою легалізацією у судових процесах, особливо коли доказ отримано з хмарних сервісів чи міжнародних джерел. Проблемою також є відсутність єдиних стандартів для збору та обробки цифрових доказів, недостатня кількість узгоджених протоколів між правоохоронними органами, експертними установами та судами, брак сучасного обладнання та програмного забезпечення у багатьох слідчих підрозділах, швидке старіння технологій: методи, актуальні кілька років тому, вже не відповідають сучасним викликам (наприклад, аналіз даних із блокчейн-систем чи хмарних платформ). Автори пропонують створення єдиної нормативної бази для цифрової криміналістики, яка б регламентувала порядок збору, збереження та використання цифрових доказів, розробку національних стандартів цифрової експертизи, що враховують міжнародний досвід (ISO/IEC 27037, NIST), інтеграцію штучного інтелекту у криміналістичні процеси для автоматизації пошуку та класифікації цифрових доказів. Приділена увага й підготовці кадрів: створення спеціалізованих навчальних програм для слідчих, прокурорів та суддів, які враховують специфіку цифрових доказів. Дослідження Колодіної та Федорової є важливим, бо воно: окреслює нову парадигму криміналістики, де цифрові докази стають центральними; підкреслює потребу у правовій модернізації та гармонізації із міжнародними стандартами; пропонує практичні шляхи вирішення проблем, що можуть стати основою для реформування криміналістичної експертизи в Україні [2 с. 378-380].

Також дослідники з Харківського національного університету внутрішніх справ у роботі «Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні» зазначають, що цифрова криміналістика є однією з найактуальніших галузей судових наук. Вони акцентують на потребі правоохоронних органів у ефективних інструментах для виявлення, вилучення та дослідження цифрових доказів. Автори підкреслюють, що цифрова криміналістика сьогодні є однією з найважливіших сфер судової експертизи, оскільки більшість злочинів має цифровий слід. Вони наголошують, що правоохоронні органи повинні мати доступ до ефективних засобів для виявлення, вилучення та дослідження цифрових доказів, адже саме ці докази часто є ключовими у розслідуванні кіберзлочинів. Цифрові артефакти (логи систем, метадані, приховані файли, інформація з мобільних пристроїв та хмарних сервісів) стають основою для встановлення істини у кримінальних провадженнях. Автори наголошують, що на практиці виникають труднощі з міжнародною співпрацею у випадках транскордонних злочинів, також багато правоохоронних органів не мають сучасного обладнання та програмного забезпечення для якісного вилучення цифрових доказів, і звертають увагу на недостатній кількості підготовлених експертів у сфері цифрової криміналістики, слідчі часто не мають спеціальних знань для роботи з цифровими доказами [3 с. 283-294].

У статті Гори І.В., Колесника В.А. та Поповича І.І. «До питання про цифрову криміналістику в системі криміналістичних знань» автори наголошують, що цифрова криміналістика сьогодні є однією з найактуальніших галузей судових наук, яка формує нову парадигму доказування у правозастосуванні. Вони підкреслюють, що сучасні злочини дедалі частіше залишають цифрові сліди, які не можуть бути виявлені традиційними методами, а отже потребують спеціалізованих інструментів та методик. Цифрові артефакти – метадані, системні журнали, залишкові файли, інформація з мобільних пристроїв та хмарних сервісів – стають ключовими джерелами доказів у кримінальних провадженнях, проте їхня допустимість у суді часто викликає дискусії через відсутність чіткої правової регламентації. Автори звертають увагу на те, що цифрова криміналістика має бути інтегрована у систему криміналістичних знань як окрема галузь, яка поєднує технічні, правові та організаційні аспекти. Вони акцентують на проблемах відсутності єдиних стандартів збору та збереження цифрових доказів, кадровому дефіциті спеціалістів, а також швидкому старінні технологій, що знижує ефективність розслідувань. Вирішення цих проблем вони вбачають у створенні нормативної бази, гармонізованої з міжнародними стандартами, у розвитку освітніх програм для слідчих, прокурорів та суддів, у впровадженні інноваційних технологій, зокрема штучного інтелекту та машинного навчання, а також у розширенні міжнародної співпраці для ефективного розслідування транскордонних кіберзлочинів. У підсумку автори доходять висновку,

що цифрова криміналістика є не допоміжним, а центральним елементом сучасної криміналістики, без якого неможливо забезпечити належний рівень протидії злочинності у цифрову епоху [4 с. 86–91].

Нові дослідження показують, що сучасні стратегії, які використовують кіберзлочинці для шахрайства з корпораціями, не мають криміналістичної рамки для виявлення та протидії таким схемам. Новітні роботи підкреслюють перспективність штучного інтелекту та предиктивної аналітики у вдосконаленні виявлення кіберзлочинів.

Сукупний огляд літератури виявляє три ключові прогалини. По-перше, бракує емпіричних досліджень, що зосереджуються саме на застосуванні цифрових криміналістичних методів у контексті розслідування кіберзлочинів. По-друге, ефективність криміналістичних інструментів не була порівняно оцінена між секторами на основі реальних даних справ. По-третє, потенційна синергія між аналітикою на основі штучного інтелекту та традиційними криміналістичними методами залишається малодослідженою.

У цьому дослідженні застосовано змішаний дизайн, що поєднує кількісні та якісні підходи, для кількісної оцінки ефективності інструментів цифрової криміналістики у розслідуванні злочинів проти підприємницької діяльності в об'єктах критичної інфраструктури.

Під час написання даної роботи було прийнято рішення звернутися за статистикою до матеріалів CERT-UA за 2024 рік, яка демонструє різке зростання кіберінцидентів в Україні – 4315 випадків проти 2541 у 2023 році (+69,8%). Це свідчить про системну активізацію кібератак, спрямованих передусім на: органи влади та урядові структури, сектор безпеки та оборони, енергетичну інфраструктуру, комерційні організації та телекомунікації. До основних типів атак належить: поширення шкідливого ПЗ, фішинг, компрометація облікових записів і систем, несанкціоновані підключення.

Мета зловмисників – викрадення чутливої інформації (зокрема даних оборонно-промислового комплексу та урядових структур) та знищення інформаційних систем.

CERT-UA підкреслює, що кібератаки є складовою війни проти України, а кіберпростір – одна з найгарячіших точок протистояння. Очікується, що рф продовжить використовувати всі можливі методи, особливо проти критичної інфраструктури (зокрема енергетики). Стаття засвідчує, що кіберзагрози для України мають стратегічний характер і постійно зростають. Ворог системно атакує критично важливі галузі, намагаючись дестабілізувати державу та отримати дані оборонного значення. Водночас Україна активно посилює кіберзахист, розвиває інституційні механізми реагування та закликає громадян до дотримання кібергігієни як елементу національної безпеки [5].

Досліджуючи дану тематику стає зрозумилим, що розслідування кіберзлочинів у сучасному світі є одним із найскладніших напрямів діяльності правоохоронних органів та спеціалізованих експертних установ. Стрімкий розвиток інформаційних технологій, глобалізація цифрових комунікацій та зростання залежності суспільства від електронних систем призвели до того, що злочинність перемістилася у віртуальний простір. Кіберзлочини охоплюють широкий спектр протиправних діянь: від банального шахрайства з банківськими картками до складних атак на критичну інфраструктуру держави. Їхня особливість полягає у високій латентності, транснаціональному характері та використанні складних технологічних інструментів, що ускладнює процес виявлення, фіксації та доведення вини конкретних осіб. Сучасні кіберзлочини мають кілька ключових рис, які визначають специфіку їхнього розслідування. По-перше, це «анонімність злочинців», яка забезпечується використанням VPN, проксі-серверів, технологій TOR, криптовалютних транзакцій та інших засобів приховування особистості. По-друге, це «транскордонність»: злочин може бути скоєний з території іншої держави, а його наслідки відчуваються у багатьох країнах одночасно. По-третє, це «динамічність технологій»: методи атак постійно змінюються, з'являються нові вектори проникнення, а традиційні інструменти захисту швидко втрачають актуальність.

Розслідування кіберзлочинів потребує застосування спеціальних методів цифрової криміналістики. Цифрова криміналістика – це галузь знань і практики, яка займається пошуком, вилученням, аналізом та збереженням цифрових доказів. Її завданням є забезпечення достовірності та допустимості доказів у суді. Важливим аспектом є те, що цифрові докази часто мають форму «невидимих слідів» – метаданих, логів системи, залишкових файлів у пам'яті пристроїв, інформації про час і місце доступу до ресурсів. Ці дані потребують спеціалізованих інструментів для вилучення та аналізу, таких як EnCase, FTK Imager, X-Ways Forensics, Wireshark, а також сучасних

систем аналізу великих даних, та спеціальних знань в правоохоронців, для належного використання даних систем та технологій.

Однією з ключових проблем у розслідуванні кіберзлочинів є «правова невизначеність». У багатьох країнах, включно з Україною, законодавство лише поступово адаптується до нових реалій. Питання допустимості цифрових доказів, їхньої автентичності та ланцюга збереження (chain of custody) залишаються дискусійними. Судові органи часто стикаються з труднощами у кваліфікації кіберзлочинів, адже традиційні норми кримінального права не завжди враховують специфіку цифрового середовища. Це створює ризик уникнення відповідальності злочинцями через процесуальні прогалини.

Ще необхідно виділити одну із основних проблем це «кадровий дефіцит». Розслідування кіберзлочинів потребує висококваліфікованих спеціалістів, які одночасно володіють знаннями у сфері інформаційних технологій, права та криміналістики. У багатьох правоохоронних органах бракує таких кадрів, що знижує ефективність розслідувань. Вирішення цієї проблеми можливе через створення спеціалізованих освітніх програм, підготовку експертів у сфері цифрової криміналістики та залучення приватних компаній до співпраці з державними структурами.

Важливим аспектом під час розслідування даної категорії справ є «міжнародна співпраця». Оскільки кіберзлочини часто мають транснаціональний характер, їхнє розслідування неможливе без взаємодії між правоохоронними органами різних країн. Інтерпол, Європол, а також спеціалізовані центри кібербезпеки створюють платформи для обміну інформацією та координації дій. Проте існують проблеми юрисдикції, адже різні країни мають різні правові режими щодо цифрових доказів та кіберзлочинів.

Особливу увагу слід приділити «розслідуванню атак на критичну інфраструктуру». Енергетичні системи, транспорт, телекомунікації та фінансові установи є найбільш уразливими до кібератак. Їхнє порушення може призвести до масштабних соціально-економічних наслідків. Розслідування таких злочинів потребує комплексного підходу: технічного аналізу, правової оцінки та стратегічної координації між державними та приватними структурами.

Не менш важливим є питання «інтеграції штучного інтелекту та машинного навчання» у процеси цифрової криміналістики. Сучасні алгоритми здатні автоматично аналізувати великі масиви даних, виявляти закономірності та прогнозувати поведінку злочинців. Це відкриває нові можливості для проактивного виявлення загроз та підвищення ефективності розслідувань. Проте використання ШІ породжує нові правові та етичні виклики, зокрема щодо прозорості алгоритмів та допустимості їхніх результатів у суді.

Таким чином, розслідування кіберзлочинів має низку особливостей, які відрізняють його від традиційних кримінальних розслідувань. Це складність технологічного середовища, анонімність злочинців, транскордонність, швидка еволюція методів атак, правова невизначеність та кадровий дефіцит. Вирішення цих проблем можливе лише через комплексний підхід, який включає розвиток цифрової криміналістики, удосконалення законодавства, міжнародну співпрацю, підготовку кадрів та впровадження інноваційних технологій.

Висновки. Підсумовуючи зазначене, приходимо до висновку, що розслідування кіберзлочинів у XXI столітті є не лише технічним завданням, а й стратегічним імперативом для забезпечення національної безпеки та економічної стабільності. Успішна протидія кіберзлочинності потребує синергії між державними органами, приватними компаніями та громадянами, адже лише спільними зусиллями можна створити ефективний захист від загроз цифрового світу.

Вважаємо за необхідне наголосити на важливості інвестувати у навчання та розвиток потенціалу: правоохоронці та криміналісти повинні проходити постійне навчання для адаптації до нових цифрових інструментів та тактик кіберзлочинності. Також варто розробити міжюрисдикційні протоколи: для подолання відмінностей у правових та технічних стандартах між країнами, слід розробити та гармонізувати міжнародні рамки поводження з цифровими доказами. На належному рівні інвестувати у криміналістичні інструменти на основі ШІ: політика та фінансування досліджень повинні підтримувати розробку та валідацію систем штучного інтелекту, здатних автоматизувати частину процесів отримання, класифікації та інтерпретації цифрових доказів.

Наслідки отриманих результатів є далекосяжними у прикладному вимірі. Криміналістичні процедури можуть бути вдосконалені, ресурси оптимально розподілені, а програми навчання оптимізовані правоохоронними органами, фахівцями з кібербезпеки та судовими інституціями, використовуючи ці результати. Дане дослідження також відкриває нові напрями для подальших

наукових пошуків. Впровадження штучного інтелекту та машинного навчання у криміналістичні процедури, кодифікація показників ефективності та розширення секторального й географічного охоплення є критичними етапами розвитку криміналістики, також підтверджує місце комп'ютерної криміналістики як основи розслідування кіберзлочинів. В епоху зростаючих цифрових загроз здатність правильно ідентифікувати, досліджувати та переслідувати злочини, що здійснюються за допомогою технологій, є не лише технічною необхідністю, а й стратегічним імперативом для національної оборони та економічного добробуту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кримінальний процесуальний кодекс України з постатейними матеріалами практики КСУ, ВСУ, Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ: наук.-практ. посіб. / за заг. ред. А.В. Столітнього. Київ : Норма права, 2020. 1504 с. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 26.11.2025).
2. Колодіна А.С., Федорова Т.С. «Цифрова криміналістика: проблеми теорії і практики». *Юридичний науковий електронний журнал.* 2022. С. 378-380. DOI: 10.32782/2524-0374/2022-4/90
3. Степанюк Р.Л., Перлін С.І. «Цифрова криміналістика й удосконалення системи криміналістичної технікив Україні». *Вісник Луганського державного університету внутрішніх справ ім. Е.О. Дідоренка.* 2022. № 3 (99). С. 283-294. DOI:10.33766/2524-0323.99.283-294.
4. Гора І.В., Колесник В.А., Попович І.І. До питання про цифрову криміналістику в системі криміналістичних знань. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2024. № 68. С. 86–91. DOI https://doi.org/10.24144/2307-3322.2024.85.4.9.
5. Полтавська обласна військова адміністрація. URL: https://poda.gov.ua/news/208531 (дата звернення: 26.11.2025).