УДК 343.98:004
https://doi.org/10.33994/kndise.2026.71.05

Падалка Андрій Миколайович

доктор юридичних наук, доцент,
начальник Департаменту господарського забезпечення
Служби безпеки України
https://orcid.org/0000-0003-1433-1030
kosto7800@gmail.com

Пашинська Ірина Володимирівна

Доктор філософії (PhD) за спеціальністю 081 «Право»,
судовий експерт Центру судових і спеціальних експертиз
Українського науково-дослідного інституту спеціальної
техніки та судових експертиз Служби безпеки України
https://orcid.org/0000-0003-0430-6667
pashynskairyna96@gmail.com

Бібліографічний опис статті: Падалка А. М., Пашинська І. В. (2026). Цифрова криміналістика як напрям розвитку судової експертизи у кримінальному провадженні. *Криміналістика і судова експертиза*, 71, 62–75. doi: https://doi.org/10.33994/kndise.2026.71.05

ЦИФРОВА КРИМІНАЛІСТИКА ЯК НАПРЯМ РОЗВИТКУ СУДОВОЇ ЕКСПЕРТИЗИ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Стаття присвячена комплексному дослідженню цифрової криміналістики як самостійного напряму розвитку судово-експертної діяльності у кримінальному провадженні в умовах стрімкої цифровізації суспільства та трансформації злочинності. Обґрунтовано, що сучасний етап розвитку інформаційних технологій супроводжується суттєвим зростанням кількості кіберзлочинів, а також ускладненням механізмів їх вчинення, що актуалізує потребу у вдосконаленні інструментарію роботи з цифровими доказами. Значну увагу приділено аналізу наукових підходів до визначення сутності цифрової криміналістики, її місця у системі криміналістики як науки та в судовій експертології. **Метою дослідження є** розгляд цифрової криміналістики як міждисциплінарного напряму, що поєднує методи криміналістики, інформаційних технологій та теорії доказів, а також виокремлення основних підгалузей цифрової форензики, зокрема комп'ютерну, мережеву, мобільну, хмарну та криптовалютну.

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

Методологічною основою роботи стали загальнонаукові та спеціальні методи дослідження, зокрема формально-логічний, системно-структурний, порівняльно-правовий та метод аналізу та узагальнення наукових джерел і практики судово-експертної діяльності. Це дозволило комплексно розглянути правові та методичні аспекти використання цифрової криміналістики як складової розвитку інформаційного забезпечення судової експертизи. **Наукова новизна** полягає у визначенні проблем розвитку цифрової криміналістики в Україні: нормативну неврегульованість дослідження та використання цифрових доказів, недостатній рівень інформаційного та технічного забезпечення експертних установ та дефіцит кваліфікованих кадрів. Особливу увагу приділено перспективам використання технологій штучного інтелекту у судово-експертній діяльності, а також пов'язаним із цим правовим викликами. У **висновках** сформульовано пропозиції щодо вдосконалення законодавства, зокрема запровадження окремої глави про цифрові докази у кримінальному процесуальному законодавстві, оновлення правового регулювання судово-експертної діяльності та розробки загальних експертних методик проведення досліджень з використанням цифрових технологій. Обґрунтовано необхідність формування єдиної методології цифрової криміналістики, що забезпечать належну доказову силу цифрових доказів у кримінальному провадженні.

Ключові слова: цифрова криміналістика, судова експертиза, кримінальне провадження, цифрові докази, комп'ютерно-технічна експертиза, електронні сліди.

Padalka Andrii

Doctor of Law, Associate Professor,
Head of the Logistics and Supply Department of the Security Service of Ukraine
https://orcid.org/0000-0003-1433-1030
kosto7800@gmail.com

Pashynska Iryna

PhD in Law (Specialty 081 "Law"),
Forensic Expert at the Center for Forensic and Special Examinations of the Ukrainian Research Institute of Special Equipment and Forensic Science of the Security Service of Ukraine
https://orcid.org/0000-0003-0430-6667
pashynskairyna96@gmail.com

DIGITAL FORENSICS AS A DIRECTION FOR THE DEVELOPMENT OF FORENSIC SCIENCE IN CRIMINAL PROCEEDINGS

To cite this article: Padalka, A., Pashynska, I. (2026). Tsyfrova kryminalistyka yak napriam rozvytku sudovoi ekspertyzy u kryminalnomu provadzhenni [Digital forensics as a direction for the development of forensic science in criminal proceedings]. *Criminalistics and Forensics, 71,* 62–75. doi: https://doi.org/10.33994/kndise.2026.71.05

The article is devoted to a comprehensive study of digital forensics as an independent direction in the development of forensic expert activity in criminal proceedings under conditions of rapid digitalization of society and the transformation of crime. It is substantiated that the current stage of information technology development is accompanied by a significant increase in cybercrime, as well as the growing complexity of its commission, which actualizes the need to improve the tools for handling digital evidence. Considerable attention is paid to the analysis of scientific approaches to defining the essence of digital forensics, its place within the system of criminalistics as a science and within forensic science. **The aim of the study** is to examine digital forensics as an interdisciplinary field that combines methods of criminalistics, information technology, and the theory of evidence, as well as to identify the main subfields of digital forensics, including computer, network, mobile, cloud, and cryptocurrency forensics. **The methodological basis** of the research includes general scientific and special methods, in particular formal-logical, system-structural, comparative-legal methods, as well as methods of analysis and generalization of scientific sources and forensic practice. This made it possible to comprehensively examine the legal and methodological aspects of the use of digital forensics as a component of the development of information support for forensic expertise. **The scientific novelty** lies in identifying the key problems in the development of digital forensics in Ukraine, including insufficient legal regulation of the examination and use of digital evidence, inadequate technical and informational support of forensic institutions, and a shortage of qualified personnel. Particular attention is paid to the prospects of using artificial intelligence technologies in forensic activities, as well as to the related legal challenges. **The conclusions** formulate proposals for improving legislation, in particular by introducing a separate chapter on digital evidence in criminal procedural law, updating the legal framework of forensic expert activity, and developing general forensic methodologies for conducting examinations using digital technologies. The necessity of forming a unified methodology of digital forensics is substantiated, which will ensure the proper evidentiary value of digital evidence in criminal proceedings.

Keywords: digital forensics, forensic science, criminal proceedings, digital evidence, computer forensic examination, electronic traces.

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

Постановка проблеми

Сучасний стан розвитку інформаційного суспільства характеризується не лише стрімким технологічним прогресом, а і якісною трансформацією злочинного середовища. Злочинці дедалі частіше використовують цифрові технології як інструмент вчинення суспільно небезпечних діянь, а цифровий простір перетворився на самостійне операційне середовище злочинної діяльності. За даними Департаменту кіберполіції України, впродовж 2022–2024 рр. кількість зареєстрованих кіберзлочинів зросла більш ніж на 40 %, тоді як відсоток їх розкриття залишається вкрай низьким — здебільшого через відсутність належного інструментарію роботи з цифровими доказами [1].

Постановка проблеми зумовлена об'єктивним протиріччям між потребами кримінального судочинства у надійному механізмі збирання та дослідження електронних доказів — з одного боку, та відставанням вітчизняної судово-експертної системи та правового регулювання від темпів цифрової трансформації — з іншого боку. Йдеться про системну невідповідність, яка проявляється одразу в трьох площинах: *нормативно-правовій* (відсутність спеціального процесуального регулювання використання цифрових доказів); *організаційно-методичній* (брак єдиної методології проведення цифрових досліджень) та *кадровій* (недостатня *спеціальна компетенці*я судових експертів у сфері цифрових технологій).

Особливої гостроти ця проблема набуває в умовах повномасштабної війни в Україні, коли фіксація воєнних злочинів та злочинів проти людяності значною мірою здійснюється через цифрові докази — відеозаписи, дані про геолокацію, метадані знімків, листування у месенджерах. Саме судова експертиза покликана надати цим матеріалам належну процесуальну форму, необхідну для їх використання у міжнародних трибуналах та національних судах. Неспроможність судово-експертної системи належно впоратися з цим завданням матиме наслідком не лише процесуальні втрати у конкретних провадженнях, а й підрив довіри до доказової бази у судових справах, що мають для України виняткове екзистенційне та міжнародне значення.

Крім того, слід констатувати, що доктринальна дискусія щодо правової природи цифрової криміналістики та її місця в системі судово-експертної діяльності ще не завершена: у науковій літературі відсутній консенсус навіть щодо базових понять, що ускладнює формування єдиної методології залучення цифрових доказів у судову практику. Це зумовлює нагальну потребу у комплексному теоретичному дослідженні, яке б синтезувало наявні наукові підходи та запропонувало загальноприйнятну концепцію використання засобів та методів цифрової криміналістики у кримінальному провадженні.

Аналіз останніх досліджень і публікацій

Проблематика цифрової криміналістики та використання електронних доказів у кримінальному провадженні перебуває в центрі уваги вітчизняної та зарубіжної наукової спільноти вже понад два десятиліття, однак особливої актуальності вона набула після 2019–2020 рр. у зв'язку з масовою цифровізацією суспільної діяльності, поширенням хмарних технологій і криптовалют, а також стрімким зростанням транснаціональної кіберзлочинності.

Серед вітчизняних науковців, що зробили визначний внесок у розробку теоретичних засад цифрової форензики, передусім слід виділити В. Ю. Шепітько, у колективній монографії за його редакцією розроблено концепцію цифрового сліду як самостійного криміналістичного об'єкта, запропоновано класифікацію електронних слідів за джерелом походження, ступенем латентності та стійкістю до знищення. Науковці переконливо доводять, що традиційні криміналістичні вчення про сліди потребують суттєвого переосмислення в контексті цифрового середовища, оскільки властивості цифрового сліду (здатність до необмеженого копіювання, транскордонний характер) принципово відрізняють його від матеріальних слідів злочину [2, с. 134].

О. М. Єськов у монографії «Цифровий доказ у кримінальному провадженні» (2021) здійснив комплексний аналіз правової природи цифрового доказу крізь призму чинного КПК України та міжнародних вимог до електронних доказів, зокрема, задекларованих у Будапештській конвенції в 2001 році. Дослідник дійшов висновку, що відсутність у КПК окремої норми, яка б визначала поняття «електронний доказ» та регламентувала спеціальний порядок його отримання, є системною прогалиною, що породжує колізії у судовій практиці. Ця позиція отримала широкий резонанс у наукових колах і стала відправною точкою для подальших дискусій щодо необхідності реформування процесуального законодавства у цій сфері [3, с. 190].

Суттєвим внеском у розвиток науки стали праці В. В. Тіщенка, присвячені методології розслідування злочинів із використанням комп'ютерних технологій. Вчений обґрунтовує необхідність виокремлення цифрової криміналістики як комплексного наукового напряму, що синтезує здобутки криміналістики, інформаційних технологій та теорії судових доказів, і пропонує авторську систему методів цифрового розслідування, побудовану за принципом технологічної нейтральності [4].

Значне місце у сучасній науковій дискусії посідають дослідження з проблем застосування штучного інтелекту в судово-експертній діяльності. Т. М. Міщенко здійснив емпіричне дослідження можливостей ШІ-систем для автоматизованого аналізу великих масивів цифрових даних у ході розслідування злочинів. Автори фіксують супе-

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

речність між технологічними можливостями таких систем і браком правових механізмів контролю за їх застосуванням у судочинстві — висновок, що нам імпонує і який, на наш погляд, окреслює один із ключових векторів подальшої законотворчої роботи [5, с. 133].

Ж. В. Удовенко дослідила проблеми підготовки судових експертів у галузі цифрових технологій, зокрема проаналізувала освітні програми провідних університетів Великобританії, Нідерландів та Польщі. Науковець дійшла висновку, що вітчизняна система підготовки судових експертів суттєво відстає від потреб практики: у навчальних планах бракує дисциплін із мережевої форензики, аналізу метаданих та роботи зі спеціалізованими апаратно-програмними комплексами. Враховуючи це, пропозиції авторки щодо реформування освітніх стандартів заслуговують на ретельне вивчення в контексті розробки нових державних стандартів вищої освіти [6, с. 142].

В аспекті нормативно-правового регулювання цифрових доказів значний науковий інтерес становлять праці Н. І. Клименко. У статті «Криміналістика і судова експертиза в цифрову епоху» (2022) вчена аналізує трансформацію предмета і методу криміналістичної науки під впливом цифрових технологій та обстоює позицію про необхідність закріплення в Законі України «Про судову експертизу» окремого розділу, присвяченого цифровим дослідженням. З цією позицією ми в цілому солідаризуємось, хоча вважаємо, що питання слід вирішувати системно — шляхом прийняття комплексних змін до КПК, Закону «Про судову експертизу» та підзаконних актів Міністерства юстиції України одночасно, а не фрагментарними поправками [7].

Серед зарубіжних авторів особливої уваги заслуговує фундаментальна праця Е. Кейсі «*Digital Evidence and Computer Crime*» (4-те вид., 2022), яка є апробованим академічним підручником у провідних університетах світу. Дослідник систематизує методологічні засади цифрової форензики, розкриває принципи ланцюга збереження доказів (*chain of custody*), обґрунтовує вимоги до відтворюваності методик цифрової форензики та визначає вимоги допустимості цифрових доказів у судочинстві різних правових систем [8, с. 11].

Таким чином, аналіз останніх наукових публікацій свідчить про те, що цифрова криміналістика сформувалася як повноцінний науковий напрям із власним предметом, методологією та інституційною інфраструктурою. Водночас у літературі фіксуються такі прогалини, як: відсутність уніфікованої термінології у вітчизняному праві, брак нових експертних методик для нових видів цифрових досліджень (хмарних ресурсів, IoT-форензика, блокчейн-форензика)[1], недостатнє теоретичне обґрунтування правового режиму алгоритміч-

1 IoT (Internet of Things) – це міжмережева взаємодія між обчислювальними пристроями, об'єктами, оснащеними мережею датчиків, приватними комп'ютерами, смартфонами та деякими необчислювальними пристроями.

них доказів. Саме ці прогалини визначають актуальність і наукову новизну пропонованого дослідження.

Мета дослідження

Метою статті є теоретико-правовий аналіз цифрової криміналістики як міждисциплінарного напряму судово-експертної діяльності, уточнення її понятійно-категоріального апарату та місця у системі судової експертизи, дослідження особливостей цифрових слідів і доказів, аналіз чинного нормативно-правового регулювання їх використання у кримінальному провадженні, а також виявлення проблем і розробка науково обґрунтованих пропозицій.

Виклад основного матеріалу

Термін «цифрова криміналістика» у вітчизняній науковій літературі не має усталеного визначення, що породжує суттєву термінологічну неузгодженість. У найбільш широкому розумінні під цифровою криміналістикою розуміють галузь знань, що охоплює методи та засоби виявлення, збереження, аналізу й документування цифрових доказів з метою їх використання у судочинстві. Зарубіжна доктрина розрізняє поняття «*computer forensics*» (комп'ютерна криміналістика), «*digital forensics*» (цифрова криміналістика) та «*cyber forensics*» (кіберкриміналістика), розглядаючи їх у відношенні загального і часткового [9].

Звертаємо увагу на позицію Н.І. Клименко, яка зазначає, що «криміналістична наука, акумулюючи досягнення суміжних наук — інформатики, кібернетики, теорії зв'язку, — формує якісно новий методологічний інструментарій для роботи з цифровими слідами злочинів». Поділяємо таку позицію, оскільки вона відображає міждисциплінарний характер цифрової криміналістики та її органічний зв'язок із традиційною криміналістичною технікою [7, с. 48].

Варто наголосити, що цифровий слід (*digital trace*) є самостійним видом криміналістичного сліду, якому притаманні специфічні властивості: латентність, мінливість, висока вразливість до знищення, можливість необмеженого копіювання без деградації інформації та транскордонний характер. Як зазначено вище, специфіка цифрового сліду визначає особливі вимоги до методики його виявлення та процесуальної фіксації [8, с. 12].

Правову основу використання цифрових доказів у кримінальному провадженні України формують кілька рівнів нормативно-правового регулювання. На конституційному рівні Основний Закон гарантує недоторканність особистого і сімейного життя, таємницю листування та іншої кореспонденції (ст. 31, 32 Конституції України), що є базовими обмеженнями під час збирання цифрових доказів.

Кримінальний процесуальний кодекс України (далі — КПК Украї-

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

їни) 2012 р. закріплює поняття речових доказів та документів (статті 98–99), фіксацію кримінального провадження (статті 103–107), а також регламентує проведення обшуку та огляду (статті 234–237) і тимчасового доступу до речей і документів (статті 159–166). Однак, як справедливо зазначають дослідники, КПК України не містить окремої глави, присвяченої цифровим доказам, і не визначає спеціальних процесуальних гарантій їх збирання і перевірки [10].

Закон України «Про судову експертизу» від 25 лютого 1994 р. № 4038-XII (зі змінами) визначає правові, організаційні та фінансові засади судово-експертної діяльності, але жодним чином не враховує цифровізацію судової експертизи на сучасному етапі її розвитку та суспільну потребу у забезпеченні судочинства можливістю експертного дослідження цифрових доказів (хмарних даних, криптовалютних транзакцій, метаданих тощо), що свідчить про необхідність його актуалізації [11].

На підзаконному рівні ключовим нормативно-правовим актом є наказ Міністерства юстиції України від 08.10.1998 р. № 53/5 «Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз» (зі змінами), який встановлює перелік видів (підвидів) судових експертиз, серед яких — комп'ютерно-технічна та телекомунікаційна та регламентує загальний порядок взаємодії слідчого (прокурора) із судовим експертом, проте не враховує специфіки цифрових досліджень, зокрема вимог до форензичного копіювання носіїв інформації [12].

У контексті міжнародно-правової регламентації поводження з цифровими доказами варто виділити Конвенцію Ради Європи про кіберзлочинність (Будапештська конвенція) 2001 р., ратифіковану Україною у 2005 р., яка зобов'язала держави-учасниці запровадити спеціальні процесуальні повноваження для збирання електронних доказів (статті 16–21). Беручи до уваги євроінтеграційний курс України, вважаємо доцільним врахувати також такий нормативно-правовий акт ЄС, як Регламент ЄС 2023/1543 про електронні докази (*e-Evidence Regulation*), який встановлює механізм транскордонного доступу до електронних даних, що зберігаються у хмарних сервісах і у провайдерів послуг, — це є вкрай актуальним в умовах розгалужених міжнародних злочинних мереж [13, с. 125].

Слід зазначити, що традиційна класифікація судових експертиз, закріплена у вітчизняному законодавстві, виокремлює комп'ютерно-технічну і телекомунікаційну експертизи як самостійний вид. Утім, розвиток інформаційних технологій зумовив появу нових різновидів цифрових досліджень, які не вкладаються в межі чинної класифікації. Погоджуємось із позицією вчених, які обстоюють необхідність виокремлення цифрової криміналістики як комплексного наукового напряму, що синтезує методи комп'ютерно-технічної,

телекомунікаційної, мережевої та мобільної форензики [2, с. 74].

З огляду на зазначене вище, у структурі цифрової криміналістики доцільно розрізняти такі підгалузі: 1) комп'ютерну форензику (дослідження жорстких дисків, файлових систем, видалених даних); 2) мережеву форензику (аналіз мережевого трафіку, журналів подій, IP-адресації); 3) мобільну форензику (дослідження смартфонів, планшетів, носіїв GPS-інформації); 4) хмарну форензику (аналіз даних, розміщених на хмарних платформах); 5) криптовалютну форензику (відстеження транзакцій у блокчейн-мережах); 6) мультимедійну форензику (автентифікація відео-, аудіо- та фотоматеріалів).

Варто звернутися до досвіду британської системи судових експертиз, де функціонує Forensic Science Regulator — незалежний регулятор у сфері судово-наукової діяльності, який видає обов'язкові стандарти проведення цифрових досліджень. Дотримання принципів ланцюга збереження доказів (*chain of custody*), відтворюваності методик та незалежності експерта є трьома фундаментальними вимогами, що забезпечують допустимість цифрових доказів [9].

Аналіз стану цифрової криміналістики в Україні дозволяє виявити низку системних проблем, що стримують її ефективний розвиток. Першою серед них є термінологічна і класифікаційна невизначеність: чинне законодавство не містить дефініцій «цифрового доказу», «електронного сліду», «метаданих» у процесуально-правовому сенсі, що породжує труднощі при оцінці допустимості таких доказів судами.

Другою ключовою проблемою є недостатній рівень матеріально-технічного забезпечення судово-експертних установ. Значна частина лабораторій не оснащена спеціалізованими апаратно-програмними комплексами для форензичного аналізу (*Cellebrite UFED*, *Oxygen Forensic Detective*, *Magnet AXIOM*), що суттєво обмежує можливості дослідження мобільних пристроїв та зашифрованих носіїв інформації.

Третьою проблемою є недостатній рівень підготовки судових експертів у галузі цифрових технологій. Як справедливо стверджує Л. М. Головченко, «сучасний судовий експерт у галузі комп'ютерно-технічної діяльності повинен мати глибокі знання не лише в юридичній, а й у технічній сфері — програмуванні, мережевих технологіях, криптографії». Враховуючи це, актуальним є запровадження спеціалізованих освітніх програм підготовки судових експертів цифрового профілю на рівні магістратури та відомчого підвищення кваліфікації [13, с. 126].

Перспективним напрямом є запровадження методів штучного інтелекту для аналізу великих масивів цифрових даних. За даними дослідження Ж. В. Удовенко, використання ШІ-систем дозволяє скоротити час аналізу даних у рамках розслідування злочинів на 60–70 % порівняно з традиційними методами. Разом із тим застосування алгоритмів штучного інтелекту в судово-експертній діяльності пору-

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

шує питання прозорості, однозначного тлумачення та відповідальності, що потребують окремого правового врегулювання.

Проведене дослідження дозволяє сформулювати висновок, що цифрова криміналістика є комплексним науково-практичним напрямом, що формується на перетині криміналістики, інформаційних технологій та теорії судових доказів. Її виникнення є об'єктивною відповіддю наукової спільноти та правозастосовної практики на виклики технологічної злочинності. Подальший розвиток цього напряму неможливий без формування самостійного понятійно-категоріального апарату, що охоплює поняття «цифровий доказ», «електронний слід», «форензичний аналіз» та інші базові категорії.

Чинне нормативно-правове регулювання залучення цифрових доказів у кримінальному провадженні України має системні прогалини, що породжують проблеми допустимості та оцінки таких доказів у судовому процесі. З метою їх вирішення пропонуємо: а) доповнити КПК України окремою главою «Цифрові докази», яка б визначала поняття, види та особливості збирання, фіксації й перевірки електронних доказів; б) внести зміни до Закону України «Про судову експертизу» в частині формалізації цифрової форензики як самостійного класу судових експертиз; в) забезпечити ратифікацію Другого додаткового протоколу до Будапештської конвенції щодо посиленого міжнародного співробітництва у сфері кіберзлочинності.

Саме місце цифрової криміналістики у судовій експертизі визначається її функцією процесуального інструменту, що забезпечує трансформацію «сирих» цифрових даних у допустимі та достовірні докази. Реалізація цієї функції потребує запровадження єдиної методології «цифрових» судово-експертних досліджень, заснованої на принципах наукової відтворюваності, технологічної нейтральності цифрової форензики та процесуальної незалежності судового експерта у частині обраних для дослідження інформаційних технологій.

Перспективи розвитку цифрової криміналістики в Україні пов'язані з трьома інноваційними напрямами: по-перше, модернізацією матеріально-технічного забезпечення судово-експертних установ та запровадженням спеціалізованих форензик-комплексів; по-друге, реформуванням системи підготовки судових експертів через запровадження магістерських програм у галузі цифрової форензики; по-третє, активізацією міжнародного співробітництва у форматі EU-Ukraine Forensic Cooperation Framework.

Враховуючи стрімкий розвиток технологій штучного інтелекту, вважаємо за доцільне розробити окрему Методику застосування систем штучного інтелекту в судово-експертній діяльності, яка б визначала умови, межі та процесуальний порядок використання алгоритмічних аналітичних інструментів при дослідженні цифрових доказів, а також гарантії прав учасників кримінального провадження.

Висновки

Проведене дослідження дозволило здійснити теоретико-правовий аналіз цифрової криміналістики як міждисциплінарного напряму судово-експертної діяльності та встановити, що вона формується на перетині криміналістики, інформаційних технологій і теорії судових доказів, виконуючи функцію трансформації цифрових даних у процесуально допустимі докази; уточнення понятійно-категоріального апарату засвідчило відсутність у національній правовій системі уніфікованих дефініцій базових категорій, що зумовлює необхідність їх нормативного закріплення; дослідження особливостей цифрових слідів і доказів дало змогу визначити їх специфічні властивості, зокрема латентність, мінливість, вразливість до знищення, можливість копіювання та транскордонність, що обумовлює особливі вимоги до їх виявлення, фіксації та дослідження; аналіз чинного нормативно-правового регулювання показав його фрагментарність і невідповідність сучасним технологічним викликам, зокрема відсутність спеціальної регламентації цифрових доказів у кримінальному процесуальному законодавстві та недостатню адаптацію законодавства про судову експертизу.

Зокрема у результаті проведеного дослідження, виявлено ключові проблеми розвитку цифрової криміналістики, серед яких термінологічна невизначеність, недосконаліть правового забезпечення, обмеженість матеріально-технічної бази та недостатній рівень підготовки експертів; з урахуванням цього обґрунтовано науково-практичні пропозиції, що полягають у необхідності нормативного закріплення інституту цифрових доказів у кримінальному процесі, удосконалення законодавства про судову експертизу, впровадження єдиної методології цифрових форензичних досліджень, розвитку спеціалізованої підготовки експертів та врахування міжнародних стандартів, що в сукупності сприятиме підвищенню ефективності використання цифрових доказів у кримінальному провадженні.

Список використаних джерел:

1. Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році. URL: https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/ (дата звернення: 12.04.2026).

2. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі : монографія / [В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін.]; за заг. ред. В. Ю. Шепітька; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. 208 с.

3. Єськов О. М. Цифровий доказ у кримінальному провадженні: правова природа та процесуальний статус. *Право і суспільство*. 2021. № 4. С. 189–197.

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

4. Тіщенко В. В. Теоретичні і практичні проблеми формування основ воєнної криміналістики. *Вісник НАПрН України*. 2023. Т. 30. № 3. С. 357–370.

5. Міщенко Т.М. (2024). Інтеграція ШІ-технологій в судово-експертну діяльність. Актуальні питання судової експертології, криміналістики та кримінального процесу : наук. матеріали VI Міжнар. наук.-практ. конф., (Київ, 20.12.2024). КНДІСЕ. Київ, 2024. С. 131-134.

6. Удовенко Ж. В. (2024). Інтеграція штучного інтелекту в кримінальне провадження. Кримінальне судочинство : сучасний стан та перспективи розвитку: матеріали Всеукр. наук.-практ. конф. (Київ, 02.05.2024). Київ: НАВС, 2024. С. 140-143. URI: https://ekmair.ukma.edu.ua/handle/123456789/29821 (дата звернення: 12.04.2026).

7. Клименко Н. І. Криміналістика і судова експертиза в цифрову епоху. *Вісник Академії адвокатури України.* 2022. Т. 19. № 1. С. 41–50.

8. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 4th ed. Academic Press, 2022. 211 p.

9. Forensic Science Regulator. Codes of Practice and Conduct for Digital Forensics. FSR-C-107. Issue 2. UK Government, 2020.

10. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 12.04.2026).

11. Про судову експертизу : Закон України від 25 лютого 1994 р. № 4038-XII. URL: https://zakon.rada.gov.ua/laws/show/4038-12 (дата звернення: 12.04.2026).

12. Про затвердження Інструкції про призначення та проведення судових експертиз : наказ Міністерства юстиції України від 08 жовтня 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98 (дата звернення: 12.04.2026).

13. Головченко Л. М. Підготовка судових експертів у галузі цифрових технологій : вимоги сучасності. *Теорія та практика судової експертизи і криміналістики.* 2022. Вип. 26. С. 117–131.

References:

1. Departament kiberpolitsii Natsionalnoi politsii Ukrainy. (2024). Zvit pro diialnist Departamentu kiberpolitsii Natsionalnoi politsii Ukrainy u 2024 rotsi [Report on the activities of the Cyberpolice Department of the National Police of Ukraine in 2024]. URL: https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/ (accessed: 12.04.2026) [in Ukrainian].

2. Shepitko V.Yu. (Ed.), Avdieieva H.K., Shevchuk V.M., et al. (2024). Innovatsiini metody ta tsyfrovi tekhnolohii v kryminalistytsi ta sudovii ekspertyzi [Innovative methods and digital technologies in criminalistics and forensic science]. Kharkiv: Pravo [in Ukrainian].

3. Yeskov O.M. (2021). Tsyfrovi dokazy u kryminalnomu provadzhenni:

pravova pryroda ta protsesualnyi status [Digital evidence in criminal proceedings: Legal nature and procedural status]. *Pravo i suspilstvo*, 4, 189–197 [in Ukrainian].

4. Tishchenko V.V. (2023). Teoretychni ta praktychni problemy formuvannia osnov voiennoi kryminalistyky [Theoretical and practical problems of forming the foundations of military criminalistics]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy*, 30(3), 357–370 [in Ukrainian].

5. Mishchenko T.M. (2024). Intehratsiia tekhnolohii shtuchnoho intelektu v sudovo-ekspertnu diialnist [Integration of artificial intelligence technologies into forensic activity]. Aktualni pytannia sudovoi ekspertyzy, kryminalistyky ta kryminalnoho protsesu: materialy VI Mizhnarodnoi naukovo-praktychnoi konferentsii, Kyiv, December 20, 2024. Kyiv: Kyivskyi naukovo-doslidnyi instytut sudovykh ekspertyz, 131–134 [in Ukrainian].

6. Udovenko Zh.V. (2024). Intehratsiia shtuchnoho intelektu u kryminalne provadzhennia [Integration of artificial intelligence into criminal proceedings]. Kryminalna yustytsiia: suchasnyi stan ta perspektyvy rozvytku: materialy Vseukrainskoi naukovo-praktychnoi konferentsii, Kyiv, May 2, 2024. Kyiv: Natsionalna akademiia vnutrishnikh sprav, 140–143. URL: https://ekmair.ukma.edu.ua/handle/123456789/29821 (accessed: 12.04.2026) [in Ukrainian].

7. Klymenko N.I. (2022). Kryminalistyka ta sudova ekspertyza v tsyfrovu epokhu [Criminalistics and forensic examination in the digital age]. *Visnyk Akademii advokatury Ukrainy*, 19(1), 41–50 [in Ukrainian].

8. Casey E. (2022). Digital evidence and computer crime: Forensic science, computers and the Internet. 4th ed. Academic Press [in English].

9. Forensic Science Regulator. (2020). Codes of Practice and Conduct for Digital Forensics (FSR-C-107, Issue 2). UK Government [in English].

10. Kryminalnyi protsesualnyi kodeks Ukrainy vid 13.04.2012 No. 4651-VI [Criminal Procedure Code of Ukraine: Law of Ukraine No. 4651-VI dated April 13, 2012]. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (accessed: 12.04.2026) [in Ukrainian].

11. Pro sudovu ekspertyzu: Zakon Ukrainy vid 25.02.1994 No. 4038-XII [On Forensic Examination: Law of Ukraine No. 4038-XII dated February 25, 1994]. URL: https://zakon.rada.gov.ua/laws/show/4038-12 (accessed: 12.04.2026) [in Ukrainian].

12. Instruktsiia pro pryznachennia ta provedennia sudovykh ekspertyz ta ekspertnykh doslidzhen: Nakaz Ministerstva yustytsii Ukrainy vid 08.10.1998 No. 53/5 [Instruction on the Appointment and Conduct of Forensic Examinations and Expert Studies: Order of the Ministry of Justice of Ukraine No. 53/5 dated October 8, 1998]. URL: https://zakon.rada.gov.ua/laws/show/z0705-98 (accessed: 12.04.2026) [in Ukrainian].

13. Holovchenko L.M. (2022). Pidhotovka sudovykh ekspertiv u sferi tsyfrovykh tekhnolohii: suchasni vymohy [Training of forensic experts

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

in the field of digital technologies: Modern requirements]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky*, 26, 117–131 [in Ukrainian].

Надійшла до редакції / Received: 15.04.2026
Отримана після доопрацювання / Received after revision: 23.04.2026
Прийнято до друку / Accepted for publication: 27.04.2026
Опубліковано / Published: 29.05.2026

Фінансування: відсутнє / Funding: none.
Конфлікт інтересів: автор(и) заявляє(ють) про відсутність конфлікту інтересів / Conflict of interest: the author(s) declare no conflict of interest.
Дотримання етичних норм: дослідження виконано з дотриманням принципів академічної доброчесності / Ethical compliance: the study was conducted in accordance with the principles of academic integrity.
Дані дослідження: усі дані, необхідні для обґрунтування висновків, наведено у статті / Research data: all data necessary to substantiate the conclusions are presented in the article.