Електронні докази у кримінальному процесі: методи їх виявлення, дослідження та правове закріплення

Валерія Шульга *[a], **Ліна Калюжна** **[b]**

* Національний університет «Полтавська політехніка імені Юрія Кондратюка», м. Полтава, Україна, ORCID: https://orcid.org/0009-0000-7239-2494, e-mail: feup.Shulha@nupp.edu.ua

** Національний університет «Полтавська політехніка імені Юрія Кондратюка», м. Полтава, Україна, e-mail: kalyuzhna1892@gmail.com

[a] Написання оригінального рукопису, адміністрування проєкту, нагляд.
[b] Написання оригінального рукопису.

DOI: 10.32353/khrife.3.2025.10 УДК 343.9:004.056.5
Надійшло 23.07.2025 / Рецензовано 04.08.2025 / Прийнято до друку 24.09.2025 / Доступно онлайн 30.09.2025

Проведено комплексний аналіз електронних доказів у кримінальному процесі, визначено їх місце та значення в системі доказів. Розглянуто сутність електронних доказів, їхню природу й особливості зберігання, фіксування й подальшого дослідження. Акцентовано на тому, що розвиток цифрових технологій створює нові можливості для збирання доказової інформації, але водночас спричиняє низку проблем, пов'язаних із допустимістю та автентичністю таких даних. Окреслено коло основних джерел електронних доказів, до яких належать комп'ютерні системи, мобільні пристрої, сервери, хмарні сервіси, цифрові камери відеоспостереження, електронні листування та інші об'єкти, що містять цифрову інформацію. Досліджено сучасні криміналістичні методи збирання електронних доказів, зокрема методи ідентифікації, фіксування та вилучення інформації з носіїв цифрових даних. Окреслено етапи та процедури, яких слід дотримувати для забезпечення збереження інформації у незміненому вигляді, що є критично важливим для подальшої її допустимості в судовому процесі. Зауважено необхідність дотримання принципів цілісності, конфіденційності й достовірності під час роботи з цифровими доказами. Окрему увагу приділено процесуальному аспекту — порядку оформлення елек-

тронних доказів відповідно до вимог кримінального процесуального законодавства України. Проаналізовано чинні норми, що регулюють процедури збирання, зберігання та надання таких доказів до суду. Виявлено основні проблеми правозастосовної практики, поміж яких — недостатнє врегулювання питань щодо збереження електронних доказів, складність підтвердження їх автентичності й ризики фальсифікації. Зазначено необхідність вдосконалення законодавчої бази та запровадження єдиних стандартів роботи з електронними доказами. Сформульовано пропозиції щодо оптимізації механізмів збирання та процесуального оформлення електронних доказів, а також упровадження сучасних технічних засобів і програмного забезпечення, яке відповідає міжнародним стандартам.

Ключові слова: *електронні докази; кримінальний процес; криміналістика; цифрові технології; збирання доказів; процесуальне оформлення; інформаційна безпека; автентичність; цифрова експертиза.*

Постановка наукової проблеми

У зв'язку із цифровізацією суспільства й активним упровадженням електронних технологій у повсякденне життя електронні докази стають важливим компонентом кримінального провадження. Їхні особливості — зокрема, нематеріальна форма, залежність від технічних носіїв і нестабільність — зумовлюють потребу у впровадженні нових методів виявлення, документування та аналізування такої інформації.

Названі особливості не лише ускладнюють процедуру процесуального оформлення електронних доказів, а й піддають сумніву автентичність і допустимість відповідних матеріалів у суді, особливо за умови порушення правил фіксування цифрових даних. Значна частина доказової інформації, отриманої з електронних джерел, потребує спеціалізованого технічного супроводу під час її збирання, для чого необхідно залучати фахівців у галузі інформаційних технологій і цифрової криміналістики.

Сьогодні в Україні відсутнє системне нормативне регулювання у кримінальній сфері, яке охоплювало б усі етапи роботи з електронними доказами: від джерела (носія) до процесуального оформлення. Кримінальний процесуальний кодекс України[1] (далі — *КПК України*) не містить ані згадки про цифрові об'єкти, ані тлумачення поняття «електронні докази». (Хоча в національному правовому полі України категорія «електронні докази» уперше отримала офіційне нормативне закріплення у 2017 році, коли відповідні положення було інтегровано до Цивільного процесуального кодексу України, Господарського процесуального кодексу України та Кодексу адміністративного судочинства України. Це стало важливим кроком у розвитку процесуального права та юридичної практики в умовах цифровізації суспільства.) Усе це спричиняє значні труднощі в діяльності експертів,

1 Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 25.06.2025).

спеціалістів, слідчих і прокурорів, а також сумніви щодо допустимості отриманих доказів у судовому процесі.

Мета статті

Здійснити комплексний науковий аналіз теоретичних і практичних аспектів застосування електронних доказів у кримінальному процесі (у межах цієї мети заплановано: визначити сутність електронних доказів; розкрити специфіку їх ідентифікації, збирання, фіксування, зберігання та аналізування для потреб криміналістики; дослідити процесуальний порядок оформлення та застосування електронних доказів у судовому провадженні з урахуванням вимог національного законодавства й міжнародних стандартів), виявити проблемні аспекти, пов'язані з правовим регулюванням, технічним забезпеченням і допустимістю електронних доказів у кримінальному провадженні, а також запропонувати науково обґрунтовані рекомендації щодо вдосконалення теорії та практики роботи з електронними доказами в умовах розвитку інформаційних технологій.

Методи дослідження

Застосовано загальнонаукові (аналіз, синтез, порівняння, моделювання) та спеціальні методи (формально-логічний, порівняльно-правовий, структурно-функціональний і криміналістичний).

Аналіз основних досліджень і публікацій

Електронні докази як об'єкт дослідження стали предметом наукових розвідок М. Гуцалюка зі співавторами [2], О. Метелева [3], В. Мурадова [4], М. Пашковського [5], В. Романюка й Т. Фоміної [6], А. Скрипника [7], А. Столітнього й І. Каланчі [8] та ін. Науковці зазначають про відсутність єдиного підходу до природи електронних доказів: більшість трактує їх як окрему категорію, дехто — як форму

2 Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / за заг. ред. О. В. Корнейка. Вид. 2-ге, допов. Київ, 2020. 104 с. URL: https://surli.cc/klrpaf (дата звернення: 25.06.2025).

3 Метелев О. П. Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства.* 2023. № 1—2. С. 42—53. DOI: 10.17721/2413-5372.2023.1-2/42-53 (дата звернення: 25.06.2025).

4 Мурадов В. В. Електронні докази: криміналістичний аспект використання. *Порівняльно-аналітичне право*. 2013. № 3-2. С. 316—318. URL: https://pap-journal.in.ua/wp-content/uploads/2020/09/3-2_2013.pdf (дата звернення: 25.06.2025).

5 Пашковський М. І. Використання електронних (цифрових) доказів у кримінальних провадженнях про колабораційну діяльність: практика судів Одеської області. *Протидія проявам тероризму та колабораціонізму в умовах війни: стан та перспективи :* мат-ли Всеукр. кругл. столу (Кропивницький, 24.11.2023). Кропивницький, 2023. С. 42—48. URL: https://surl.lt/wpqxyo (дата звернення: 25.06.2025).

6 Романюк В. В., Фоміна Т. Г. Порядок збирання електронних (цифрових) доказів у кримінальних провадженнях про колабораційну діяльність. *Вісник Кримінологічної асоціації України*. 2024. Т. 32. № 2. С. 344—353. DOI: 10.32631/vca.2024.2.25 (дата звернення: 25.06.2025).

7 Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія. Харків, 2022. 408 с.

8 Столітній А. В., Каланча І. Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. 2019. Вип. 146. С. 179—191. DOI: 10.21564/2414-990x.146.171218 (дата звернення: 25.06.2025).

фіксування даних, що підлягають класифікації за вже визначеними джерелами (документами, речовими доказами, показаннями, висновками експертів); а також зауважують дефіцит нормативного визначення процедур вилучення та фіксування цифрових даних. Аналізування судової практики репрезентує нестійкий підхід до допустимості електронних доказів, що часто зумовлено помилками на етапі їх вилучення, недотриманням вимог до фіксування, невизначеністю джерела тощо.

Особливо проблемним у цьому контексті є з'ясування особи, яка мала доступ до інформації, у якому цифровому середовищі цю інформацію створили або змінили та як саме вона потрапила до слідчих органів. Ідентифікація суб'єкта доступу до цифрових даних і джерела їх походження залишається одним з найскладніших завдань у роботі з електронними доказами. Електронні докази потрібно розглядати у зв'язку з технічними умовами їх створення, автентичності та процесуального забезпечення — насамперед, через слідчі дії (обшук, огляд, тимчасовий доступ), а не як абстрактну правову категорію.

Викладення основного матеріалу дослідження

У сучасному кримінальному процесі електронні докази набувають усе більшого значення як інструмент фіксування та підтвердження обставин правопорушення. Їхня специфічна природа потребує не лише застосування спеціальних технічних засобів для збирання та аналізування інформації, а й нормативного закріплення їхнього процесуального статусу як самостійного виду доказів у межах кримінального процесуального законодавства. У контексті кримінального провадження доказами визнають фактичні дані, які здобуто в чітко визначеному процесуальному порядку та на підставі яких уповноважені суб'єкти кримінального процесу — слідчий, прокурор, слідчий суддя або суд — мають змогу дійти висновків про наявність або відсутність обставин, що мають правове значення для з'ясування істини у справі. Таке визначення містить ст. 84 КПК України, де також закріплено вичерпний перелік процесуальних джерел доказів [9]. Зокрема, законодавець називає такими джерелами показання учасників кримінального процесу, речові докази, документи, висновки експертів [10].

Згідно зі ст. 98 КПК України, речовими доказами можуть визнавати будь-які матеріальні об'єкти, якими послуговувалися як засобами вчинення кримінального правопорушення та які зберегли на собі його сліди або містять відомості, що мають доказове значення для з'ясування обставин злочину. До таких предметів можуть належати об'єкти, що стали об'єктом злочинного посягання, а також грошові кошти, цінності й інші речі, здобуті злочинним шляхом. У цьому розумінні речові докази відіграють важливу роль як матеріальна база, що забезпечує перевірку й оцінювання інших джерел доказової інформації [11].

Особливе місце у структурі доказової інформації посідають документи, які, відповідно до ст. 99 КПК України, можуть визнати речовими доказами за умови, що вони містять відомості, релевантні для визначення юридично

9 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 16.07.2025).

10 Там само.

11 Там само.

значущих фактів. У цій нормі законодавець акцентує увагу на тому, що документами визнають як традиційні матеріальні носії інформації, так і сучасні електронні засоби фіксування — зокрема, фотографії, відео- й аудіозаписи, а також інші носії, створені і/або збережені за допомогою комп'ютерної техніки. До того ж окремі документи, що характеризуються незмінністю форми та змісту, можуть мати подвійний статус — одночасно документа й речового доказу [12].

Згідно з викладеним вище, електронні докази у кримінальному провадженні слід розглядати як специфічну форму доказової інформації, яка існує в цифровому (нематеріальному) форматі та підлягає фіксуванню, збереженню, опрацюванню й оцінюванню з урахуванням як технічних, так і правових аспектів [13].

З огляду на це, такі докази можна отримати за допомогою комп'ютерних пристроїв, серверів, цифрових носіїв інформації або з мережевих джерел — зокрема, із інтернету. Проте для подальшого застосування в доказуванні така інформація потребує спеціального програмного або технічного опрацювання, яке забезпечує її перетворення в доступну для сприйняття форму.

У сучасній правозастосовній практиці паралельно з терміном «електронні докази» часто послуговуються терміном «цифрові докази» (англ. *digital evidence*). Через відсутність нормативного закріплення та чіткого розмежування цих понять, їх нерідко застосовують як синоніми, хоча окремі дослідники пропонують їх розрізняти відповідно до контексту — наприклад, «електронні» як формально-процесуальна категорія, а «цифрові» — як технічна характеристика носія [14].

Згідно із Законом України «Про електронні документи та електронний документообіг», будь-яку інформацію, подану у формі, придатній для її опрацювання електронними засобами, уважають даними. Такі дані можуть мати юридичне значення і, за умови належного фіксування, посвідчення автентичності та збереження цілісності, ними послуговуються як доказами у кримінальному провадженні [15].

Із технічного боку, зберігання таких доказів можливе на/у різноманітних цифрових носіях: зовнішніх пристроях (зокрема, на картах пам'яті, жорстких дисках, мобільних телефонах); внутрішніх або зовнішніх серверах; хмарних сховищах або системах резервного копіювання; віртуальному середовищі інтернету. Усе це формує нову доказову реальність, у якій значна частина інформації, що має юридичне значення, існує винятково в цифровому вигляді [16].

Свого часу ми зазначали, що (незважаючи на відсутність чіткого визначення в КПК України) цифрові докази стали невід'ємною складовою судових розглядів. Застосування їх розширює можливості доказування, але потребує особливої уваги до питань автентич-

12 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 16.07.2025).

13 Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Зазнач. твір. URL: https://surli.cc/klrpaf (дата звернення: 25.06.2025).

14 Там само.

15 Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 22.07.2025).

16 Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. Зазнач. твір. URL: https://surli.cc/klrpaf (дата звернення: 25.06.2025).

ності та допустимості. Для забезпечення балансу між інтересами правосуддя та захистом прав людини необхідно розробити докладні правила доказування на підставі цифрових даних [17].

Окрім того, А. Назарко вважає головним завданням удосконалення законодавчого підґрунтя у сфері застосування електронних доказів, оскільки чинна правова база значно відстає від сучасних викликів цифровізації й ускладнює ефективне застосування таких доказів у кримінальному провадженні [18].

Законом від 23.02.2024 р. № 3604-IX Верховна Рада України внесла зміни до КПК України щодо поетапного впровадження Єдиної судової інформаційно-комунікаційної системи. Закон передбачає застосування електронного документообігу, фіксування кримінального провадження технічними засобами й подання процесуальних документів в електронній формі. Попри те, що він не дає прямого визначення поняття «електронні докази», він створює підґрунтя для формалізації їх застосування у кримінальному процесі — зокрема, за допомогою модулів електронного суду і відеоконференції [19].

Отже, названі підходи свідчать про пильну увагу до електронних даних як до самостійного виду доказів у кримінальному провадженні, що обумовлює необхідність законодавчо врегулювати їх процесуальний статус.

Викладене вище суголосне висновкам А.-М. Ангеленюк про необхідність нормативного закріплення чіткого понятійного апарату щодо електронних доказів у кримінальному процесі, оскільки відсутність законодавчого визначення та унормованої процедури обігу цифрових даних зумовлює колізії у правозастосовній практиці, що своєю чергою спричиняє ризики порушення принципів допустимості й належності доказів. Науковиця також зауважує невизначеність меж між електронним носієм і джерелом доказової інформації, що потребує чітких доктринальної та процесуальної конкретизацій [20].

Так, у низці судових рішень, які ми проаналізували у процесі цього дослідження, сформульовано критерії прийнятності окремих видів електронних даних як доказів у кримінальному провадженні. Наприклад, аудіозапис телефонної розмови, здійснений автоматично (за допомогою постійно активної програми на пристрої власника), визнають допустимим доказом. Водночас аудіозапис, зроблений із задумом

17 Шульга В. Правові аспекти застосування цифрових доказів у кримінальному процесі. *Діджиталізація судово-експертної науки в умовах воєнного стану* : зб. мат-лів Міжнар. наук.-практ. конф. (Харків, 08.11.2024). Харків, 2024. С. 408—410. URL: https://surl.li/czlrua (дата звернення: 25.06.2025).

18 Nazarko A. E-Evidence in Ukrainian Criminal Justice: Exploring the Legal Realities and Theoretical Perspectives. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 80. Ч. 2. С. 183—188. DOI: 10.24144/2307-3322.2023.80.2.28 (дата звернення: 26.06.2025).

19 Про внесення змін до Кримінального процесуального кодексу України щодо забезпечення поетапного впровадження Єдиної судової інформаційно-комунікаційної системи : Закон України від 23.02.2024 р. № 3604-IX. URL: https://zakon.rada.gov.ua/laws/show/3604-20#Text (дата звернення: 26.06.2025).

20 Ангеленюк А.-М. Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання). *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 79. Ч. 2. С. 214—218. DOI: 10.24144/2307-3322.2023.79.2.32 (дата звернення: 25.06.2025).

зафіксувати розмову, суд оцінює як недопустимий доказ через порушення вимог процесуального законодавства [21].

Можна дійти висновку, що брак чіткого законодавчого регламентування, невизначеність термінології та нерозмежованість носія і джерела електронної інформації спричиняють неоднакове тлумачення судами електронних доказів. Допустимість аудіозаписів часто залежить не від технічних характеристик, а від дотримання процесуальних норм їх отримання. Це свідчить про те, що юридична формалізація має не менше значення, аніж технічна достовірність. Аналогічна ситуація з відеозаписами, де провідну роль відіграє спосіб отримання. Для забезпечення єдності правозастосування та дотримання принципів справедливого процесу необхідно нормативно врегулювати порядок обігу, допустимості й належності електронних доказів у кримінальному провадженні.

Особливості криміналістичного збирання електронних доказів зумовлені специфікою їх походження, зберігання і способів передавання. Найчастіше такі докази існують у вигляді цифрових слідів — *IP*-адрес, *log*-файлів, електронної переписки, медіафайлів або метаданих, які мають значення для кримінального провадження. Їх цінність для слідства полягає у можливості з'ясувати факти, пов'язані з особою правопорушника, місцем, часом і способом скоєння злочину [22].

У практиці європейських країн, зокрема Франції, Німеччини, Португалії та Швеції, електронні докази формально прирівнюють до традиційних письмових доказів. Водночас більшість національних законодавств не містить окремого нормативного визначення поняття «електронний доказ», натомість послуговуються науковими дефініціями або загальними процесуальними положеннями. Незважаючи на відсутність єдиного підходу, країни ЄС демонструють прагнення уніфікувати практику збирання, зберігання й обміну цифровими доказами [23].

Окрім національного законодавства, важливу роль у регулюванні питань збирання електронних доказів відіграють міжнародно-правові акти. Поміж них варто виокремити Європейську конвенцію про взаємодопомогу у кримінальних справах 1959 року [24], яка заклала фундаментальні принципи міжнародної співпраці у сфері кримінального судочинства, зокрема щодо отримання доказів за межами національної юрисдикції. Особливе значення в контексті електронних доказів має Будапештська конвенція про кіберзлочинність 2001 року [25]. Цей документ став першим і до сьогодні залишається основним міжнародним дого-

21 Ангеленюк А.-М. Зазнач твір. DOI: 10.24144/2307-3322.2023.79.2.32 (дата звернення: 25.06.2025).

22 Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : монографія. Львів, 2022. 204 с. URL: https://surl.li/kdsnwm (дата звернення: 20.07.2025).

23 Там само.

24 Європейська конвенція про взаємну допомогу у кримінальних справах : Конвенція Ради Європи від 20.04.1959 р. ; ратифік. із заяв. і застереж. Закон. України від 16.01.1998 р. № 44/98-ВР (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/995_036#Text (дата звернення: 22.07.2025).

25 Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 р. ; ратифік. із заяв. і застереж. Закон. України від 07.09.2005 р. № 2824-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 22.07.2025).

вором, спрямованим на врегулювання питань боротьби з кіберзлочинністю (зокрема, шляхом уніфікації процедур фіксування, збирання, зберігання та передавання цифрових слідів).

Будапештська конвенція передбачає механізми співпраці між державами для забезпечення ефективного розслідування злочинів, пов'язаних із застосуванням інформаційних технологій. Вона також обумовлює процесуальні інструменти для негайного збереження комп'ютерних даних, доступу до комп'ютерних систем і їх обшуку, вилучення інформації, перехоплення даних у режимі реального часу тощо. Такий підхід спрямований на подолання викликів, пов'язаних із глобальним характером цифрових доказів, їхньою вразливістю до змін або знищення та складністю транснаціональної взаємодії між правоохоронними органами різних країн. Отже, міжнародне нормативне підґрунтя створює необхідні умови для ефективного та правомірного збирання електронних доказів у межах кримінального провадження, допомагає долати юридичні бар'єри у сфері міжнародної співпраці.

Головними особливостями криміналістичного збирання електронних доказів є технічна складність їх виявлення, потреба в участі фахівців у галузі інформаційних технологій, а також необхідність дотримання процесуальних гарантій під час їх фіксування та опрацювання. Оперативність, цілісність і автентичність електронного доказу залишаються провідними критеріями для його допустимості в судовому процесі.

В. Романюк і Т. Фоміна слушно зауважують, що після повномасштабного вторгнення рф на територію України особливого значення набули ефективне фіксування та правове забезпечення доказової бази щодо колаборантів, левова частка дій яких відбувається в цифровому просторі. Автори зауважують, що кількість кримінальних проваджень, пов'язаних із колабораціонізмом, залишається високою, що зумовлює нагальну потребу в удосконаленні методик збирання доказів. Важливо, що у цьому разі чималий масив доказової інформації має електронну форму, оскільки діяльність колаборантів зафіксовано, зокрема, у соціальних мережах, месенджерах, на інформаційних платформах окупаційної влади тощо [26].

Окрему увагу дослідники приділили термінологічній неоднозначності у науковій і правозастосовній практиці: «електронні докази», «цифрові докази», «електронні (цифрові) докази», «електронні відображення», самі послуговуючись для позначення інформації, яку можна здобути з різноманітних електронних джерел — як відкритих (інтернет, ЗМІ, соціальні мережі), так і закритих (месенджери, комп'ютери, флешки), узагальненим терміном «електронні (цифрові) докази» [27]. Водночас у КПК України, як ми зазначали вище, не передбачено відповідного окремого поняття.

Наведені науковцями приклади із практики ілюструють, що електронні докази нерідко здобувають шляхом огляду сторінок у соціальних мережах (*Facebook, Telegram, Tik-Tok, Youtube, Viber* та ін.), а також мобільних пристроїв підозрюваних. Докази фіксують за допомогою скриншотів, відеозаписів екрана, копіювання даних, що дає змогу суду

26 Романюк В. В., Фоміна Т. Г. Зазнач. твір. DOI: 10.32631/vca.2024.2.25 (дата звернення: 29.06.2025).

27 Там само.

визнавати такі протоколи належними й допустимими доказами [28].

Цифрова інформація, як справедливо наголошено у цьому дослідженні, є вкрай уразливою з позицій її доказового статусу через легкість підроблення, модифікації або цілковитого знищення. Саме ця специфічна характеристика зумовлює необхідність максимально ретельного, стандартизованого і фахового підходу до її фіксування та зберігання. На думку М. Пашковського, яку поділяють й інші дослідники цифрової криміналістики, вирішальне значення у забезпеченні належності, допустимості й автентичності таких доказів має дотримання міжнародно визнаних протоколів, зокрема *Berkeley Protocol* [29].

Як зазначає науковець, практика українських органів досудового розслідування, на жаль, демонструє невиконання мінімального обсягу технічних процедур, передбачених цим протоколом. Здебільшого обмежуються створенням скриншотів як основної форми візуалізації цифрового контенту. Водночас ігнорують необхідність збереження вихідного *HTML*-коду вебсторінок, мультимедійних укладень, прихованих або вбудованих файлів, метаданих і *Hash*-значень, які дають змогу ідентифікувати й перевірити автентичність цифрового об'єкта. За *Berkeley Protocol*, відсутність цієї інформації є суттєвим недоліком у процедурі документування цифрових слідів, що може піддати сумніву достовірність зібраних доказів у судовому процесі [30].

Окрім того, проаналізовані вироки часто не містять згадки про здійснення вебархівування джерел, із яких вилучено цифрові докази. Між тим, застосування спеціальних інструментів вебархівування (наприклад, засобів створення зафіксованих знімків, вебресурсів у часі) є важливою гарантією того, що представлена сторінка дійсно мала певний вигляд у момент огляду й не зазнала змін після вилучення даних. Своєю чергою чітка невизначеність цієї процедури послаблює доказову цінність здобутої інформації та створює ризики для реалізації принципу змагальності в суді.

Отже, викладені у праці М. Пашковського міркування, які продовжують логіку аналізування В. Романюка та Т. Фоміної, свідчать про серйозну потребу в нормативному й методичному переосмисленні підходів до опрацювання електронних доказів в умовах сучасної війни. Українське кримінальне процесуальне законодавство, попри окремі позитивні зрушення (зокрема, визнання комп'ютерних даних документами за ст. 99 КПК України [31]), потребує подальшої деталізації процесуальних гарантій щодо способів збирання, фіксування та збереження цифрової інформації.

У цьому контексті інтегрування міжнародних стандартів (зокрема, *Berkeley Protocol*) у національну правоза-

28 Романюк В. В., Фоміна Т. Г. Зазнач. твір. DOI: 10.32631/vca.2024.2.25 (дата звернення: 29.06.2025).

29 Пашковський М. І. Зазнач. твір. С. 46. URL: https://surl.lt/wpqxyo (дата звернення: 25.06.2025) ; Berkeley Protocol on Digital Open Source Investigations / Human Rights Center, Un. Nat. Human Rights Office of the High Commissioner. New York and Geneva, 2022. 102 p. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (дата звернення: 25.06.2025).

30 Berkeley Protocol … . URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (дата звернення: 25.06.2025).

31 Кримінальний процесуальний кодекс … . URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 16.07.2025).

стосовну практику видається не лише бажаним, а й критично необхідним. Їх упровадження дасть змогу не лише забезпечити автентичність і достовірність електронних доказів, а й захистити результати досудового розслідування від оскарження в суді через порушення процесуального порядку отримання доказової інформації.

Зважаючи на те, що законодавче регулювання електронного доказування в Україні перебуває на етапі становлення, а чинне кримінальне процесуальне законодавство не містить однозначно сформульованих норм, які комплексно визначали б порядок подання, збирання, збереження та оцінювання цифрових доказів, на тлі відсутності системного нормативного підходу особливого значення набуває етап досудового розслідування. Саме в його межах відбувається первинне документування цифрової інформації, яке може ініціювати як сторона обвинувачення, так і сторона захисту, що обумовлює подальшу допустимість таких доказів у суді.

У своїх дослідженнях Р. Малюга аналізує різноманітні наукові підходи до розуміння сутності процесу збирання доказів. Зокрема, він зазначає, що деякі дослідники розглядають це як діяльність, спрямовану на виявлення, фіксування, вилучення та збереження доказової інформації. Інші акцентують увагу на ширшому тлумаченні, уважаючи, що до процесу збирання належать також дослідження й аналізування отриманих доказів. Існує також позиція, згідно з якою окремі етапи — виявлення, пошук і фіксування — є самостійними стадіями в загальній системі доказування. Дехто також висловлює думку, що збирання доказової бази охоплює всі дії від моменту виявлення потенційно значущої інформації до її належного документування [32].

Виявлення доказів є первинним етапом їх збирання та полягає в цілеспрямованому пошуку або зверненні уваги на події, обставини чи матеріальні об'єкти, які можуть містити інформацію, значущу для кримінального провадження. Найчастіше таке виявлення відбувається в межах слідчих (розшукових) заходів. Р. Малюга, ґрунтуючись на положеннях теорії відображення, пояснює, що докази мають природу слідів, які залишаються після вчинення кримінального правопорушення та зберігаються в матеріальному середовищі [33].

Збирання доказів, що мають форму електронного документа, полягає у виявленні й належному фіксуванні його матеріального носія — якщо такий фізично існує, або в забезпеченні доступу до цифрового середовища, де зберігається відповідна інформація. Це може бути сервер, хмарне сховище або інтернет-ресурс, і сам такий доступ розглядають як процес отримання електронного доказу. Своєю чергою електронні документи може зібрати слідчий, дізнавач або прокурор у межах кримінального провадження в різні процесуальні способи, зокрема, шляхом: добровільного надання такої інформації учасником провадження, витребування необхідних матеріалів, застосування тимчасового доступу до відповідних даних як заходу забезпечення, а також у результаті проведення слідчих (розшукових) дій (наприклад, огляду або обшуку) або

32 Малюга Р. В. Доказування в кримінальному процесі: проблеми визначення структурних елементів. *Наукові записки Львівського університету бізнесу та права*. 2013. Вип. 11. С. 280—283. URL: http://nbuv.gov.ua/UJRN/Nzlubp_2013_11_71 (дата звернення: 16.07.2025).

33 Там само.

в межах негласних слідчих (розшукових) заходів [34].

Слідчий або дізнавач може отримати електронний документ під час обшуку, огляду або на підставі заяви чи клопотання учасника провадження. Особі обов'язково роз'яснюють право на добровільну видачу документів. Навіть у разі добровільної видачі під час обшуку, обшук доцільно продовжити, оскільки можливе приховування інших важливих для справи предметів [35].

Утім, у КПК України й інших нормативних актах відсутні чіткі правила щодо порядку долучення електронних доказів, а також форми та змісту документів, що підтверджують їх долучення. Незазначення способу отримання або долучення доказів може призвести до їх визнання недопустимими. Наприклад, суд може відхилити як доказ протокол огляду предметів (фотографій), оскільки матеріали справи не містили інформації про те, як ці фотографії отримав слідчий [36].

Отже, процес виявлення та збирання електронних доказів має складну багаторівневу структуру, яка передбачає як технічний, так і процесуальний компоненти. Успішність фіксування й подальшого застосування таких доказів значною мірою залежить від дотримання форми, способу отримання та документального оформлення. Водночас відсутність чітких процесуальних вимог щодо процедури долучення цифрових матеріалів створює ризик їх визнання недопустимими, що прямо впливає на ефективність досудового розслідування.

Це твердження дає змогу перейти до докладного аналізування особливостей процесуального оформлення електронних доказів, зокрема документального підтвердження їх автентичності та джерела походження.

Отже, фіксування факту добровільного передавання документів винятково у протоколі огляду або обшуку створює ризики подальшого визнання відповідного доказу недопустимим. У випадку з електронними документами їх належне долучення до матеріалів провадження слід здійснювати на підставі поданої учасником провадження заяви або клопотання про долучення такого документа, що зберігається на фізичному носії інформації. Водночас факт передавання електронного документа доцільно фіксувати технічними засобами відеозапису, особливо якщо його видача відбувається в межах слідчих дій, які підлягають обов'язковому відеофіксуванню (наприклад, під час обшуку або огляду).

У межах досудового розслідування учасник кримінального провадження має право добровільно надати докази, зокрема електронні документи, винятково слідчому, дізнавачеві або прокуророві, і лише в межах чинного кримінального провадження. Позиція щодо цього знайшла підтвердження і в судовій практиці: суд касаційної інстанції підтримав висновки апеляційного суду про те, що диск із відеозаписом з камер спостереження магазину, що став підставою для обвинувального вироку судом першої інстанції, отримала неуповноважена посадова особа — опера-

34 Малюга Р. В. Зазнач. твір. URL: http://nbuv.gov.ua/UJRN/Nzlubp_2013_11_71 (дата звернення: 16.07.2025).

35 Чаплинський К. О. Тактика проведення окремих слідчих дій : монографія. Дніпропетровськ, 2006. 416 с. URL: https://surl.li/wwpdti (дата звернення: 20.06.2025).

36 Вирок Ленін. райсуду м. Харкова від 01.12.2015 р. Справа № 642/6283/15-к. Провадж. № 1-кп/642/531/15 / ЄДРСР : вебсайт. URL: http://reyestr.court.gov.ua/Review/53911255 (дата звернення: 20.07.2025).

тивний працівник. Це відбулося до моменту внесення відомостей до Єдиного реєстру досудових розслідувань і з порушенням процесуальних вимог, що своєю чергою виключає можливість визнати такий доказ допустимим. Отже, доводи сторони обвинувачення щодо законності отримання цього доказу є безпідставними [37].

Як зазначає В. Вапнярчук, доцільно виокремити кілька категорій суб'єктів, від яких можна витребувати або отримати докази у кримінальному провадженні [38].

Категорії суб'єктів збирання електронних доказів (за В. Вапнярчук)

I категорія	II категорія	III категорія
Сторони й інші учасники процесу, які подають відповідну інформацію з метою реалізації своїх процесуальних прав та обов'язків, що своєю чергою дає їм змогу впливати на перебіг і результати процесуальної діяльності відповідно до власних інтересів	Державні органи, установи, організації, а також підприємства, зокрема ті, що здійснюють оперативно-розшукову діяльність. Відповідно до законодавчих норм, які визначають їх правовий статус, вони зобов'язані надавати докази в межах кримінального провадження	Інші особи, зокрема ті, що не є учасниками кримінального процесу. Вони можуть добровільно надати доказову інформацію, однак чинне законодавство не покладає на них такого обов'язку — ця дія радше має характер морального зобов'язання

У практиці досудового розслідування трапляються випадки, коли слідчі дійсно складають постанови та надсилають їх відповідним органам з метою отримати необхідні документи. Проте, як свідчить практика, здебільшого на ці постанови або взагалі не реагують, або відмовляють у наданні запитуваних матеріалів [39].

А. Коваленко акцентує увагу на особливостях процесуального оформлення огляду електронних документів, розміщених у мережі «Інтернет»:

1. Обов'язково фіксувати технічні параметри пристрою, за допомогою якого здійснюють доступ до вебресурсів, зокрема — серійний номер службового комп'ютера, назву та версію операційної системи, а також програмного забезпечення (браузера), яким послуговувався уповноважений суб'єкт під час огляду.
2. Важливо забезпечити масштабування вебсторінки до 100 % для відображення її повного змісту, а також вимкнути всі браузерні надбудови та плагіни, здатні спотворити вигляд інтернет-сторінки.

37 Постанова Верховного Суду від 07.09.2019 р. Справа № 607/14707/17. Провадж. № 51-2604км19 / ЄДРСР : вебсайт. URL: http://reyestr.court.gov.ua/Review/83589933 (дата звернення: 20.07.2025).

38 Вапнярчук В. В. Витребування та отримання, проведення інших процесуальних дій як способи збирання доказів у кримінальному провадженні. *Науковий вісник Херсонського державного університету. Серія: Юридичні науки*. 2015. Вип. 3. Т. 3. С. 85—89. URL: https://surl.lu/slaknh (дата звернення: 20.07.2025).

39 Ухвала Київ. райсуду м. Полтави від 01.04.2024 р. Справа № 552/1823/24. Провадж. № 1-кс/552/707/24 / ЄДРСР : вебсайт. URL: https://reyestr.court.gov.ua/Review/118037105 (дата звернення: 20.07.2025) ; Ухвала Яворів. райсуду Львів. обл. від 24.02.2023 р. Справа 944/1269/22. Провадж. № 1-кс/944/155/23 / Там само. URL: https://reyestr.court.gov.ua/Review/109184568 (дата звернення: 20.07.2025).

3. У протоколі огляду доцільно занотовувати всі мультимедійні матеріали, прикріплені до публікації, із зазначенням гіперпосилань на кожний з них. Водночас елементи, які не мають відношення до змісту публікації (наприклад, рекламні банери), опису не потребують.
4. Оглянуту вебсторінку необхідно роздрукувати за допомогою службового принтера, обов'язково зазначивши у протоколі його серійний номер, марку й модель. Цей роздрукований матеріал додають до протоколу як перший додаток. Усі релевантні мультимедійні файли потрібно зберегти на цифровому носії — диску, що стає другим додатком до процесуального документа. Як альтернативний спосіб фіксування вебконтенту автор пропонує зберігати сторінку у форматі **.html* безпосередньо за допомогою браузера (із подальшим перенесенням цього файлу на диск) [40].

Як зазначає Є. Хижняк, головним ідентифікатором електронного документа, розміщеного в мережі «Інтернет», є його доменна адреса, а також унікальне посилання на конкретну вебсторінку, що містить матеріали, важливі для кримінального провадження. У протоколі огляду вебресурсу обов'язково зазначено стандартні реквізити документа:

- назва,
- автор,
- дата створення (за наявності),
- призначення,
- стислий зміст.

Одним зі способів фіксування таких електронних доказів є вилучення серверів, де їх зберігають. Зокрема, *log*-файли, що містять інформацію про передавання даних, можна отримати від інтернет-провайдерів та інших власників відповідних технічних засобів [41].

Отже, у сучасній науковій літературі електронні докази дедалі частіше розглядають як окреме явище кримінального процесу, однак українські науковці акцентують увагу на необхідності чіткого розмежування між формою фіксування доказів і джерелом доказів як таким.

Зокрема, А. Столітній та І. Каланча обґрунтовано підкреслюють, що терміном «електронні докази» слід послуговуватися винятково як теоретичною категорією, оскільки чинне законодавство не виокремлює електронної форми як самостійного джерела доказів. Автори наголошують: джерела доказів залишаються незмінними — показання, речові докази, документи й висновки експертів, натомість електронна форма є лише способом їх фіксування в межах кримінального процесу [42].

Окрім того, дослідники звертають увагу на дуалістичну природу електронної інформації — її нематеріальний характер потребує обов'язкового фіксування на матеріальному носії для за-

40 Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. *Вісник Національної академії правових наук України.* 2017. № 1 (88). С. 182—191. URL: https://surl.li/qulfww (дата звернення: 20.07.2025).

41 Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. *Держава та регіони. Серія: Право.* 2017. № 4 (58). С. 80—85. URL: https://surl.li/xdtcgp (дата звернення: 25.06.2025).

42 Столітній А. В., Каланча І. Г. Зазнач. твір. DOI: 10.21564/2414-990x.146.171218 (дата звернення: 25.06.2025).

безпечення зберігання, передавання та процесуального оформлення. У цьому контексті вони обґрунтовано критикують спроби виокремити електронні докази як нову класифікаційну групу, що суперечить логіці кримінального процесу та є штучним явищем, яке не поділяє ані КПК України, ані загальноєвропейська практика [43].

Отже, електронні докази — це не окрема категорія доказів, а зафіксована на електронному носії інформація, яка відповідає одному з чотирьох законодавчо визначених джерел доказів і яку слід розглядати в контексті процесуального оформлення, а не змістовного наповнення.

Висновки

З огляду на проведене дослідження можна стверджувати, що електронні докази в умовах сучасного кримінального провадження набувають самостійного значення як інструмент виявлення та фіксування обставин, які мають юридичну вагу. Їхні цифрова природа, залежність від технічного середовища, динамічність і вразливість до змін потребують від учасників кримінального процесу не лише технологічної обізнаності, а й поводження з такими доказами відповідно до чітко регламентованих процесуальних механізмів.

Виявлення, вилучення, дослідження та належне оформлення електронних доказів слід здійснювати з урахуванням криміналістичних особливостей їх існування, а також вимог доказового права. Практика свідчить, що недотримання таких вимог призводить до втрати цифровою інформацією доказової сили, навіть за її очевидної цінності для розслідування. Це своєю чергою загрожує порушенням принципів змагальності та справедливого судового розгляду.

Аналізування наукових підходів і судових рішень дає змогу дійти висновку про недостатню визначеність у кримінальному законодавстві правової природи електронних доказів. Однак безумовним залишається те, що такі об'єкти не можна розглядати окремо від їхнього носія та технічного контексту. Саме тому головним викликом для кримінального процесу є забезпечення поєднання процесуальної форми та технічної достовірності електронних доказів.

Проведене дослідження підтвердило, що електронні (цифрові) докази сьогодні є не лише актуальним, а й критично значущим інструментом кримінального процесуального доказування. Їх поява трансформувала традиційне уявлення про джерела доказів, водночас загострившись потребу в адаптуванні процесуальних норм до умов цифрової реальності.

Зауважено, що вітчизняне кримінальне процесуальне законодавство поки не забезпечує цілісного регламентування всіх стадій опрацювання електронних доказів: від їх виявлення та фіксування до оцінювання та допустимості в суді. Відсутність чіткого визначення поняття, правового статусу й належної процедури долучення цифрових доказів суттєво ускладнює правозастосування та створює ризики процесуальних помилок.

Водночас світова практика демонструє ефективні підходи до розв'язання цих проблем за допомогою уніфікації технічних стандартів, закріплення обов'язкових процедур фіксування (зокрема, вебархівування, збереження метаданих, хешування), а також залучення *IT*-фахівців на етапі збирання та аналізування цифрових слідів.

43 Столітній А. В., Каланча І. Г. Зазнач. твір. DOI: 10.21564/2414-990x.146.171218 (дата звернення: 25.06.2025).

На підставі викладеного запропоновано розглядати електронні докази не як окрему класифікаційну групу, а як особливу форму фіксування фактичних даних, що потребує нормативної конкретизації. Головними умовами ефективного застосування електронних доказів у кримінальному процесі мають стати: формалізація їх правового статусу, визначення єдиної термінології, закріплення чіткої процедури отримання, зберігання та долучення, а також запровадження міжнародних технічних стандартів (зокрема, *Berkeley Protocol*).

Тож успішна інтеграція електронних доказів у національну систему кримінального провадження залежить від синхронного вдосконалення законодавства, методології та технічного забезпечення. Це стане запорукою забезпечення принципів змагальності, допустимості й належності доказів, отже, і справедливого судового розгляду.

Electronic Evidence in Criminal Procedure: Methods for Detecting, Investigating, and Legally Consolidating It

Valeriia Shulha, Lina Kaliuzhna

The paper presents a comprehensive analysis of electronic evidence in the context of criminal procedure. Its place and significance within the evidence system were determined. The authors highlight the essence of electronic evidence, its nature and peculiarities of storage, recording, and further investigation. Emphasis is placed on the fact that development of digital technologies opens up new possibilities for collecting evidence. Conversely, it also leads to problems related to the admissibility and authenticity of such data. The article outlines the main sources of electronic evidence, including computer systems, mobile devices, servers, cloud services, video surveillance cameras, e-correspondence and other objects that contain digital information. Current forensic methods of collecting electronic evidence, including methods of identification, recording and extraction of information from physical media, were studied. Stages and procedures that must be followed to ensure information remains unaltered—crucial for its admissibility in a trial—were outlined. The authors stress the need to conform to the principles of integrity, confidentiality and credibility when working with digital evidence. The procedural aspect was given particular attention: the procedure for formalizing electronic evidence in compliance with the requirements of Ukraine's criminal procedural legislation. Current rules governing the procedures for collection, storage and provision of such evidence in court were analyzed. The main issues in law enforcement practice include insufficient regulation of issues regarding the preservation of electronic evidence, the difficulty of establishing its authenticity, and the risk of falsification. The study underscores the importance of improving legislative framework and introducing uniform standards for working with electronic evidence. The paper outlines proposals to optimize the collection and processing of electronic evidence, and to introduce modern technical means and software that comply with international standards.

Keywords: *electronic evidence; criminal procedure; criminalistics; digital technologies; evidence collection; procedural formalization; information security; authenticity; forensic digital examination.*

Фінансування

Це дослідження не отримало жодного спеціального гранту від фінансових установ у державному, комерційному або некомерційному секторах.

Відмова від відповідальності

Засновники не грали жодної ролі у розробленні дослідження, добиранні й аналізуванні даних, рішенні про публікацію або підготовку рукопису.

Учасники

Авторки зробили свій внесок винятково в інтелектуальну дискусію, що є основою цього документа, дослідження судової практики, написання та редагування, і беруть на себе відповідальність за її зміст і тлумачення.

Декларація щодо конфлікту інтересів

Авторки заявляють, що у них відсутній конфлікт інтересів.

References

Anheleniuk, A.-M. (2023). Vykorystannia elektronnykh dokaziv u kryminalnomu protsesualnomu pravi Ukrainy (problemni pytannia) [The use of electronic evidence in the criminal procedural law of Ukraine (problematic issues)]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo.* Vyp. 79. Ch. 2. DOI: 10.24144/2307-3322.2023.79.2.32 [in Ukrainian].

Chaplynskyi, K. O. (2006). *Taktyka provedennia okremykh slidchykh dii* [Tactics for conducting individual investigative actions] : monohrafiia. Dnipropetrovsk. URL: https://surl.li/wwpdti [in Ukrainian].

Hutnyk, A. V., Khytra, A. Ya. (2022). *Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv u dokazuvanni* [Criminal procedural and forensic foundations of using electronic documents in proving] : monohrafiia. Lviv. URL: https://surl.li/kdsnwm [in Ukrainian].

Hutsaliuk, M. V., Havlovskyi, V. D., Khakhanovskyi, V. H. ta in. (2020). *Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh* [Application of electronic (digital) evidence in criminal proceedings] : metod. rek. / za zah. red. O. V. Korneika. Vyd. 2-he, dopov. Kyiv. URL: https://surli.cc/klrpaf [in Ukrainian].

Khyzhniak, Ye. C. (2017). Osoblyvosti ohliadu elektronnykh dokumentiv pid chas rozsliduvannia kryminalnykh pravoporushen [Peculiarities of the digital document review during the investigation of criminal offenses]. *Derzhava ta rehiony. Seriia: Pravo.* № 4 (58). URL: https://surl.li/xdtcgp [in Ukrainian].

Kovalenko, A. V. (2017). Osoblyvosti taktyky ohliadu elektronnykh dokumentiv pid chas dosudovoho rozsliduvannia posiahan na zhyttia ta zdorov'ia zhurnalista [The Features of Tactics of Inspection of Electronic Documents During the Pretrial Investigation of Infringements on the Life and Health of a Journalist]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy*. № 1 (88). URL: https://surl.li/qulfww [in Ukrainian].

Maliuha, R. V. (2013). Dokazuvannia v kryminalnomu protsesi: problemy vyznachennia strukturnykh elementiv [Proving in criminal proceedings: issues in defining structural components]. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava.* Vyp. 11. URL: http://nbuv.gov.ua/UJRN/Nzlubp_2013_11_71 [in Ukrainian].

Metelev, O. P. (2023). Tsyfrovi dokazy u kryminalnomu protsesi: vydova kharakterystyka [Digital evidence in criminal procedure: typological characteristic]. *Visnyk kryminalnoho sudochynstva*. № 1—2. DOI: 10.17721/2413-5372.2023.1-2/42-53 [in Ukrainian].

Muradov, V. V. (2013). Elektronni dokazy: kryminalistychnyi aspekt vykorystannia [Digital Evidence: Criminalistical Aspects of Using]. *Porivnialno-analitychne pravo.* № 3-2. URL: https://pap-journal.in.ua/wp-content/uploads/2020/09/3-2_2013.pdf [in Ukrainian].

Nazarko, A. (2023). E-Evidence in Ukrainian Criminal Justice: Exploring the Legal Realities and Theoretical Perspectives. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo.* Vyp. 80. Ch. 2. DOI: 10.24144/2307-3322.2023.80.2.28.

Pashkovskyi, M. I. (2023). Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh pro kolaboratsiinu diialnist: praktyka sudiv Odeskoi oblasti [Employing digital (electronic) evidence in criminal proceedings on collaborative activities: court practice in the Odessa region]. *Protydiia proiavam teroryzmu ta kolaboratsionizmu v umovakh viiny: stan ta perspektyvy* : mat-ly Vseukr. kruhl. stolu (Kropyvnytskyi, 24.11.2023). Kropyvnytskyi. URL: https://surl.lt/wpqxyo [in Ukrainian].

Romaniuk, V. V., Fomina, T. H. (2024). Poriadok zbyrannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh

pro kolaboratsiinu diialnist [Procedure for collecting electronic (digital) evidence in criminal proceedings concerning collaborative activities]. *Visnyk Kryminolohichnoi asotsiatsii Ukrainy*. T. 32. № 2. DOI: 10.32631/vca.2024.2.25 [in Ukrainian].

Shulha, V. (2024). Pravovi aspekty zastosuvannia tsyfrovykh dokaziv u kryminalnomu protsesi [Legal Aspects of Using Digital Evidence in Criminal Proceedings]. *Didzhytalizatsiia sudovo-ekspertnoi nauky v umovakh voiennoho stanu* : zb. mat-liv Mizhnar. nauk.-prakt. konf. (Kharkiv, 08.11.2024). Kharkiv. URL: https://surl.li/czlrua [in Ukrainian].

Skrypnyk, A. V. (2022). *Vykorystannia tsyfrovoi informatsii v kryminalnomu protsesualnomu dokazuvanni* [Use of digital information in the process of proving within criminal procedure] : monohrafiia. Kharkiv [in Ukrainian].

Stolitnii, A. V., Kalancha, I. H. (2019). Formuvannia instytutu elektronnykh dokaziv u kryminalnomu protsesi Ukrainy [Formation of the institute of electronic evidence in the criminal process of Ukraine]. *Problemy zakonnosti.* Vyp. 146. DOI: 10.21564/2414-990x.146.171218 [in Ukrainian].

Vapniarchuk, V. V. (2015). Vytrebuvannia ta otrymannia, provedennia inshykh protsesualnykh dii yak sposoby zbyrannia dokaziv u kryminalnomu provadzhenni [Requesting and Receiving, Other Procedural Actions as a Means of Gathering Evidence in Criminal Proceedings]. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Seriia: Yurydychni nauky.* Vyp. 3. T. 3. URL: https://surl.lu/slaknh [in Ukrainian].

Шульга, В., Калюжна, Л. (2025). Електронні докази у кримінальному процесі: методи їх виявлення, дослідження та правове закріплення. *Теорія та практика судової експертизи і криміналістики*. Вип. 3 (40). С. 136—152. DOI: 10.32353/khrife.3.2025.10.