

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

КАЛАНЧА ІНГА ГЕОРГІЇВНА

УДК 343.14:004(477)

ДИСЕРТАЦІЯ

ДОКАЗИ ЕЛЕКТРОННОЇ ФОРМИ У КРИМІНАЛЬНОМУ ПРОЦЕСІ
УКРАЇНИ: ТЕОРІЯ ТА ПРАКТИКА

12.00.09 – кримінальний процес та криміналістика; судова експертиза;
оперативно-розшукова діяльність

081 Право

Подається на здобуття наукового ступеня доктора юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело. Всі частини тексту дисертації, під час написання яких використовувалися технології штучного інтелекту, перевірені та відредаговані особисто

_____ **І.Г. Каланча**

Київ – 2025

АНОТАЦІЯ

Каланча І. Г. Докази електронної форми у кримінальному процесі України: теорія та практика. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. – Національна академія внутрішніх справ, Київ, 2025.

У дослідженні реалізовано доктринальний підхід до обґрунтування концептуальних засад інституту доказів електронної форми у кримінальному процесі України, визначенні їх процесуальну природу, особливості джерел походження, порядку ідентифікації, збирання, здобуття, процесуальної фіксації, зберігання і використання, а також у розробленні організаційно-практичних підходів до вдосконалення кримінального процесуального регулювання діяльності суб'єктів кримінального провадження щодо роботи з такими доказами в умовах глобальної цифровізації.

Обґрунтовано, що електронна складова кримінального процесу України складається з п'яти елементів: електронне кримінальне провадження; оцифрування матеріалів кримінальних проваджень та їх резервне зберігання; докази електронної форми; електронні інструменти доказування; електронні інструменти реалізації повноважень суб'єктів правозастосування.

Аргументовано, що «цифровий доказ» відповідає змісту доказу, «електронний доказ» – технічному способу його реалізації, а «доказ електронної форми» – процесуальній формі подання.

Визначено передумови становлення інституту доказів електронної форми в кримінальному процесі України зумовлені як технологічним розвитком, що збільшив обсяг електронних даних у кримінальних провадженнях, так і внутрішньою потребою кримінальної процесуальної науки висвітлити власне бачення нової цифрової реальності. Становлення відповідного інституту характеризується конкуренцією доктринальних підходів (від ототожнення з документами чи речовими доказами до пропозицій їх виокремлення як

самостійного процесуального джерела доказів) та значною термінологічною варіативністю. Попри широку теоретичну основу, що склалась завдяки зусиллям вітчизняних учених, вбачається потреба їх переосмислення як самостійного інституту.

Доведено, що процесуальна природа доказів електронної форми у кримінальному процесі полягає у можливості їх потенційної приналежності до всіх процесуальних джерел доказів, визначених ст. 84 КПК України. Факт належності доказу досліджуваної категорії до певного процесуального джерела визначає процесуальний порядок поводження з ними під час кримінального провадження та, як наслідок, критерії оцінки його допустимості.

Технічна природа доказів електронної форми визначено сукупністю характеристик інформаційного середовища, у якому вони створюються та зберігаються, а також властивостями електронних носіїв інформації, що досліджуються під час кримінального провадження. Доказ електронної форми функціонує як чотирирівнева структура: контент, метадані, системна оболонка та електронний носій інформації, що має матеріальне вираження. Висвітлено технічні аспекти доказів досліджуваної категорії: метадані; розмежування логічного копіювання і побітового копіювання; гешування; електронний підпис та електронна позначка часу. Гешування забезпечує ідентифікацію цифрового об'єкта та виявлення будь-яких змін, слугуючи технічною основою для підтвердження цілісності та незмінності комп'ютерних даних.

Розроблено комплекс алгоритмів, що пропонується як три стратегії фіксації доказів електронної форми у кримінальному процесі України: фізичне вилучення електронних носіїв інформації або комп'ютерних систем; огляд та копіювання комп'ютерних даних; огляд та фіксація інформації з відкритих джерел.

Обґрунтовано практично значущі механізми, що застосовуються для досягнення цієї мети систематизовано за ступенем зростання рівня надійності та визначити як: упакування та маркування електронних носіїв інформації; фіксація загальних та унікальних апаратних ідентифікаторів; опис структури і змісту комп'ютерних даних та їх метаданих; гешування комп'ютерних даних і послідовної

фіксації контрольних сум комп'ютерних даних в процесуальних документах; використання кваліфікованого електронного підпису та електронної позначки часу. Системне дослідження концепції chain of custody, її організаційно-технічних моделей, засвідчило необхідність її подальших досліджень та перспективу інституціоналізації.

Ефективність оперування доказами електронної форми у кримінальному процесі України визначається організаційною спроможністю інституцій кримінальної юстиції. Організаційну готовність суб'єктів кримінального провадження до роботи з доказами електронної форми доцільно розглядати через три взаємопов'язані компоненти: матеріально-технічний; кадровий; нормативний.

Системно досліджено процесуальні повноваження та функціональні ролі суб'єктів кримінального провадження у взаємодії з доказами електронної форми: слідчого, прокурора, захисника, слідчого судді та суду, експерта та спеціаліста.

Роль слідчого у роботі з доказами електронної форми визначено системоутворювальною. Ефективність такої діяльності передбачає поєднання правових навичок із базовою цифровою грамотністю: розуміння природи комп'ютерних даних і метаданих, механізмів логічного захисту та гешування, відмінностей між логічним і побітовим копіюванням, а також практичне володіння інструментами OSINT для оперативного виявлення релевантних слідів.

Прокурор у кримінальному провадженні виступає ключовим суб'єктом забезпечення належного обігу доказів електронної форми, поєднуючи координацію дій слідчого, оперативних підрозділів, спеціаліста й експерта контроль за дотриманням критеріїв належності, допустимості й достовірності. Його обов'язки охоплюють правомірний вибір способу одержання відомостей (копіювання інформації чи вилучення носія інформації), фіксацію ідентифікаційних параметрів комп'ютерних даних (зокрема геш-значень) у протоколах, перевірку автентичності електронних документів і електронних підписів, організацію відкриття матеріалів досудового розслідування стороні захисту відповідно до ст. 290 КПК України, а також використання механізмів міжнародної взаємодії.

Захисник у кримінальному провадженні виступає самостійним суб'єктом доказової діяльності щодо доказів електронної форми, реалізуючи гарантоване ч. 2 ст. 22 та ч. 3 ст. 93 КПК України право на їх використання. Ефективність цієї діяльності зумовлюється поєднанням процесуальної активності з технічною спроможністю забезпечити автентичність і цілісність цифрових даних (згідно ДСТУ ISO/IEC 27037:2017). На стадії обшуку й відкриття матеріалів іншій стороні (ст. 290 КПК України) пріоритетними є: мінімізація втручання у приватне життя, охорона адвокатської таємниці, вимога надання криміналістичних (побітових) копій і контрольних ідентифікаторів, а також процесуальне реагування на процесуальні порушення.

Слідчий суддя та суд формують єдиний контур процесуального контролю за доказами електронної форми: перший – через попереднє санкціонування втручання у цифрове середовище і визначення обмежень щодо цифрових пристроїв, другий – через дослідження доказів електронної форми та перевірку їх належності, допустимості, достовірності та достатності.

Процесуальна роль експерта фокусується на науково вивіреному дослідженні, використанні атестованих методик та формулюванні висновку експерта. Спеціаліст виконує технічну функцію DEFR: ідентифікація, фіксація, збереження та первинний аналіз цифрових слідів відповідно до ДСТУ ISO/IEC 27037:2017, із процесуальною фіксацією його участі й результатів. Вказано на необхідність чіткого розмежування компетенцій цих суб'єктів кримінального провадження.

Протокол Берклі розглядається як цілісна методологія роботи з даними з відкритих джерел, поєднуючи правові, етичні й технічні стандарти (ідентифікація джерел, належне збирання, збереження, перевірка, документування ланцюга збереження). Для українського кримінального процесу його імплементація забезпечує підвищення доказової якості OSINT-матеріалів, мінімізує ризики недопустимості та відповідає вимогам безпеки учасників провадження. Водночас наявний розрив між практикою «буквального» використання терміна «Протокол Берклі» й реальним дотриманням його вимог, а також відсутність у КПК України

уніфікованого порядку роботи з даними відкритих джерел, зумовлюють потребу нормативної деталізації.

Доведено, що Конвенція про кіберзлочинність визначає процесуальну модель міждержавної взаємодії щодо роботи з доказами електронної форми. В КПК України частково імплементовано ці інструменти, однак зберігаються ключові прогалини. Другий додатковий протокол поглиблює співпрацю (прямі звернення до провайдерів, прискорені процедури, надзвичайні ситуації, стандарти захисту даних) і задає вектор вдосконалення КПК України.

Обґрунтовано, що ISO/IEC 27037:2012, інтегрований у Європі як EN ISO/IEC 27037:2016 та імплементований в Україні через ДСТУ ISO/IEC 27037:2017, формує методологічне ядро поводження з доказами електронної форми: ідентифікація, збирання, здобуття (створення образу) та збереження із забезпеченням цілісності, відтворюваності й верифікованості. Українська правозастосовна практика, попри наявність вказаного ДСТУ, стикається з нормативною лакуною КПК України щодо розмежування процесів ідентифікації, збирання та здобуття доказів електронної форми, процесуального закріплення ролей DEFR та DES, фіксації ланцюга збереження тощо.

Порівняльний аналіз зарубіжного досвіду засвідчує, що докази електронної форми перетворилися на системоутворювальний елемент кримінального провадження, а ефективність їх використання зумовлюється поєднанням чітких процесуальних рамок, інституційної спроможності та транснаціональної взаємодії.

Доведено, що удосконалення організаційних засад роботи з доказами електронної форми є важливим чинником адаптації кримінального процесу України до цифрової доби. Ефективність цього напряму визначається рівнем матеріально-технічного забезпечення суб'єктів кримінального провадження, наявністю кваліфікованих кадрів і спроможністю до міжвідомчої взаємодії. Підготовка спеціалізованих кадрів, створення криміналістичних ІТ-лабораторій, а також впровадження міждисциплінарних програм навчання формують основу

інституційної спроможності системи кримінальної юстиції. Стандартизація діяльності суб'єктів кримінального провадження через розроблення стандартних операційних процедур забезпечує єдність практики, передбачуваність дій і зменшує ризики втрати доказів.

Запропоновано узгоджений підхід до процесуального вдосконалення роботи з доказами електронної форми передбачає розвиток нормативної бази зі збереженням балансу між правовою визначеністю та технічною адаптивністю, запобіганням надмірній формалізації процедур і, водночас, гарантуванням автентичності, цілісності і допустимості доказів цієї категорії. Запропоновані зміни до КПК України передбачають поетапне впровадження Конвенції про кіберзлочинність та європейських актів. Поетапне запровадження відповідних положень має супроводжуватися навчанням суб'єктів кримінального провадження, формалізації стандартних операційних процедур і створенням механізмів міжвідомчої координації.

Обґрунтовано потребу технічного вдосконалення роботи з доказами електронної форми спрямоване на ефективне використання таких доказів та потребує створення інфраструктури, що охоплює сертифіковані системи ідентифікації та зберігання.

Розроблено концепцію вдосконалення інституту доказів електронної форми у кримінальному процесі України спрямована на створення єдиного, науково обґрунтованого та технологічно інтегрованого механізму їх процесуального обігу. Її сутність полягає у комплексному розвитку нормативних, організаційних, інфраструктурних, техніко-криміналістичних, освітніх та науково-аналітичних напрямів.

Ключові слова: кримінальний процес, докази електронної форми, ISO/IEC 27037:2012, ідентифікація, здобуття, гешування, цілісність, Протокол Берклі, Конвенція про кіберзлочинність, кібербезпека, цифрові технології, бази даних, стандартні операційні процедури, електронні докази, цифрові докази.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

Монографія

1. Каланча І. Г. Докази, що мають електронну форму, в кримінальному процесі України: концептуальний аспект : монографія. Київ : Вид-во «SBA Print», 2025. 528 с.

Рецензія: Цимбал Г. П. Рецензія на монографію Каланчі Інги Георгіївни «Докази, що мають електронну форму, в кримінальному процесі України: концептуальний аспект». *Європейський правничий часопис*. №10. С. 11–13.

Публікації у виданнях, які включено до наукометричних баз Scopus і

Web of Science:

1. Patreliuk D., Svoboda I., Kalancha I., Filashkin V., Kachmar B. Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations. *Pakistan Journal of Life and Social Sciences*. 22(2). 2024. pp. 4811–4820. URL: <https://www.scopus.com/pages/publications/85204286465>.

2. Kozii V.; Kalancha I.; Vlasova H.; Orlean A. Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies. *IDP. Internet, Law an Politics Journal*. no. 42. 2025. pp. 1-13. URL: <https://www.scopus.com/pages/publications/85217974797>.

3. Kalancha I., Bozhyk V., Muzychenko O., Vatsiyk V. Digital evidence in comparative criminal procedure: international experience and the practice of judicial review. *TPM – Testing, Psychometrics, Methodology in Applied Psychology*. Vol. 32, No. S2. 2025. pp. 34-46. URL: <https://www.scopus.com/pages/publications/105013864919>.

Публікації у фахових періодичних виданнях України (категорія «Б»):

1. Каланча І. Г. Електронний сегмент в кримінальному процесуальному

законі Азербайджану. *Науковий вісник Ужгородського національного університету. Серія «Право»*. № 59. 2019. С. 117–121. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2020/12/No.59-2.pdf>.

2. Каланча І. Г. Електронний сегмент кримінального процесу Естонії. *Порівняльно-аналітичне право*. № 3. 2019. С. 212–216. URL: https://pap-journal.in.ua/wp-content/uploads/2021/07/3_2019.pdf.

3. Столітній А. В., Каланча І. Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. Вип. 146. 2019. С. 179–191. URL: <https://doi.org/10.21564/2414-990x.146.171218>.

4. Каланча І. Г. Електронний сегмент в кримінальному процесі Грузії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. № 4. 2019. С. 161–166. URL: <https://doi.org/10.31733/2078-3566-2019-4-161-166>.

5. Каланча І. Г. Роль правових актів Європейського суду з прав людини в кримінальному процесі України. *Проблеми законності*. Вип. 150. 2020. С. 233–243. URL: <https://doi.org/10.21564/2414-990x.150.209071>.

6. Каланча І. Г. Тенденції та динаміка застосування практики Європейського суду з прав людини під час кримінального провадження: статистичне та соціологічне дослідження. *Теорія і практика правознавства*. Вип. 2(18). 2020. С. 1–17. URL: <https://doi.org/10.21564/2225-6555.2020.18.213676>.

7. Каланча І. Г. Поняття практики Європейського суду з прав людини як джерела кримінального процесуального права України. *Вісник кримінального судочинства*. № 2. 2020. С. 8–21. URL: <https://doi.org/10.17721/2413-5372.2020.3-4/8-21>.

8. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Туркменістану. *Актуальні проблеми вітчизняної юриспруденції*. № 1. 2020. С. 91–95. URL: http://apnl.dnu.in.ua/1_2020/23.pdf.

9. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Вірменії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. № 1. 2020. С. 205–210. URL: <https://visnik.dduvs.edu.ua/index.php/visnyk/issue/view/48/19>.

10. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Латвії. *Криміналістика і судова експертиза : міжвідомчий науково-методичний збірник*. Вип. 65. 2020. С. 90–100. URL: https://digest.kndise.gov.ua/wp-content/uploads/2025/07/2020_65.pdf.
11. Каланча І. Г., Гаркуша А. М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*. № 8. 2021. С. 336–339. URL: <https://doi.org/10.32782/2524-0374/2021-8/77>.
12. Каланча І. Г., Орлеан А. М. Адаптація системи кримінальної юстиції до цифровізації світу: роль навчального компоненту. *Наукові перспективи*. № 11(53). 2024. С. 937–944. URL: [https://doi.org/10.52058/2708-7530-2024-11\(53\)-937-944](https://doi.org/10.52058/2708-7530-2024-11(53)-937-944).
13. Каланча І. Г., Юрчишин Ю. В. Забезпечення безпеки прокурора під час роботи з електронним сегментом кримінального провадження в Україні. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки*. Том 35 (74) № 6. 2024. С. 108–115. URL: <https://doi.org/10.32782/TNU-2707-0581/2024.6/19>.
14. Каланча І. Г. Алгоритм електронного кримінального провадження. *Law. State. Technology*. Вип. 4. 2024. С. 69–74. URL: <https://doi.org/10.32782/LST/2024-4-13>.
15. Каланча І. Г. Практика роботи з доказами, що мають електронну форму в кримінальному процесі України: соціологічне дослідження. *Успіхи і досягнення у науці*. № 1 (11). 2025. С. 76–93. URL: [https://doi.org/10.52058/3041-1254-2025-1\(11\)-76-93](https://doi.org/10.52058/3041-1254-2025-1(11)-76-93).
16. Каланча І. Г., Стемковський Д. Б. Використання доказів, що мають електронну форму в кримінальному процесі України: судова практика. *Аналітично-порівняльне правознавство*. № 2. 2025. С. 1001–1008. URL: <https://doi.org/10.24144/2788-6018.2025.02.148>.
17. Каланча І. Г. Електронний висновок експерта як доказ у кримінальному процесі України: практика, перспективи та ризики. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. № 2. 2025. С. 84–92.

URL: <https://doi.org/10.32782/2311-8040/2025-2-12>.

18. Каланча І. Г. Процесуальна природа доказів, що мають електронну форму в кримінальному процесі України: документ та речовий доказ. *Міжнародний науковий журнал "Інтернаука". Серія: "Юридичні науки"*. № 7. 2025. С. 85–92. URL: <https://doi.org/10.25313/2520-2308-2025-7-11208>.

19. Каланча І. Г. Організаційні аспекти роботи з доказами, що мають електронну форму в кримінальному процесі України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. Вип. 90. Ч. 4. 2025. С. 258–266. URL: <https://doi.org/10.24144/2307-3322.2025.90.4.36>.

Публікації у періодичних виданнях іноземних держав:

1. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законодавстві Молдови. *Jurnalul Juridic National: teorie si practica*. № 1 (41). 2020. С. 132–137. URL: <http://www.jurnaluljuridic.in.ua/archive/2020/1/30.pdf>.

2. Каланча І. Г. Інтероперабельність як обов'язкова властивість електронних інформаційних систем органів кримінальної юстиції. *Ročenka Ukrajinsko-Slovenská. Zborník vedeckých prác*. (Рочник Українсько-Словацький. Збірник наукових праць) 2020. С. 64–70. URL: <https://www.eeda.sk/dok/publikacie/ostatne/2020-rocenka-ukrajinsko-slovenska.pdf>.

3. Каланча І. Г. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світлі концепції chain of custody. *Věda a perspektivy*. № 8 (51). 2025. С. 206–230. URL: [https://doi.org/10.52058/2695-1592-2025-8\(51\)-206-230](https://doi.org/10.52058/2695-1592-2025-8(51)-206-230).

Тези виступів на науково-практичних конференціях:

1. Каланча І. Г. Єдине електронне інформаційне поле органів кримінальної юстиції. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : матер. міжн. наук.-практ. конф. (м. Київ, 05.11.2019 р.).

Київ, 2019. С. 209–213. URL: https://www.researchgate.net/publication/393743748_Kalanca_IG_Edine_elektronne_in_formacijne_pole_organiv_kriminalnoi_usticii_Aktualni_pitanna_sudovoi_ekspertologii_kriminalistiki_ta_kriminalnogo_procesu_mat_mizn_nauk-prakt_konf_m_Kiiv_5112019_r_K_2019.

2. Каланча І. Г. Шляхи формування сучасних практичних компетентностей у випускників правничих шкіл України. *Інноваційні рішення в сучасній науці, освіті та практиці*: матеріали І Міжнародної науково-практичної інтернет-конференції (наукове видання), 17–18 листопада 2020 р.: у 2 ч. Київ: НТУ, 2020. Ч. 2. С. 209–212. URL: <http://vstup.ntu.edu.ua/conf-innov-part-2.pdf>.

3. Гаркуша А. М., Каланча І. Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи*: матеріали круглого столу (м. Львів, 11 червня 2021 р.). Львів: Львівський державний університет внутрішніх справ., 2021. С. 159–165. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/11_06_2021.pdf.

4. Каланча І. Г. Підходи до класифікації електронних носіїв інформації та інформаційних систем для завдань кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: матеріали V Міжнар. наук.-практ. конф. (29 жовтня 2021 р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2021. С. 211–213. URL: <https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk-29.10.21.pdf>.

5. Гаркуша А. М., Каланча І. Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. *Наукові читання пам'яті Ганса Гросса*: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 9 грудня 2021 р.). Чернівці: Технодрук, С. 72–75. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/11383/Forensic_Epistemology_Czernowitz_2021_.pdf?sequence=1&isAllowed=y.

6. Каланча І. Г. Окремі аспекти діяльності прокурора щодо гарантування

цілісності доказів, що мають електронну форму під час досудового розслідування кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: матеріали VI Міжнар. наук.-практ. конф. (21 жовтня 2022р., Чернівці)/ редкол.: О. В. Щербанюк та ін. Чернівці, 2022. С. 327–332. URL: https://ccu.gov.ua/sites/default/files/suchasni_vyklyky_ta_aktualni_problemy_sudovoyi_reformy_v_ukrayini_2022.pdf.

7. Каланча І. Г. Способи ідентифікації комп'ютерних даних як доказу в кримінальному провадженні. *III Наукові читання пам'яті Ганса Гросса* : збірник тез міжнар. науково-практичної конференції (м. Чернівці, 8 грудня 2023 р.). Чернівці: Чернівець. нац. у-нт ім. Ю.Федьковича, 2023. С. 71–75. URL: <https://www.ndekc.cv.ua/wp-content/uploads/2024/03/III-Naukovi-chytannya-pam-yati-Gansa-Grossa.pdf>.

8. Каланча І. Г. Стратегії фіксації доказів, що мають електронну форму для застосування в кримінальному провадженні. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VII Міжнар. наук.-практ. конф. (27 жовтня 2023 р., Чернівці)/ редкол.: О. В. Щербанюк та ін. Чернівці: 2023. С. 253–258. URL: https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk_conf_27..pdf.

9. Каланча І. Г. Кіберпростір як територія проведення досудового розслідування. *Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини*: зб. наук. праць за матер. Круглого столу, Київ, 7 грудня 2023 р. / редкол.: А. Ю. Нашинець-Наумова, Г. П. Власова, С. В. Бобровник, Т. О. Дідич, Н. А. Сергієнко, А. П. Чернега. Київ : Київ. стол. ун-т ім. Б. Грінченка, 2024. С. 115–119. URL: <https://kubg.edu.ua/struktura/pidrozdili/yurydychna-klinika-astreya/zakhody/8438-ikh-kruhlyi-stil-prava-liudyny-v-umovakh-voiennoho-stanu-v-ukraini.html>.

10. Каланча І. Г. Цифрова складова кримінального процесу України в науці та практиці: структурно-функціональний аналіз. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VIII Міжнар. наук.-практ. конф. (31 жовтня 2024р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2024. С. 229–233. URL:

https://www.researchgate.net/publication/390005117_Kalanca_IG_Cifrova_skladova_kriminalnogo_procesu_Ukraini_v_nauci_ta_praktici_strukturno-funkcionalnij_analiz_Sucasni_vikliki_ta_aktualni_problemi_sudovoi_reformi_v_Ukraini_Materiali_VIII_Miznar_nauk-p.

11. Каланча І. Г. Матеріальна форма існування як властивість доказу в кримінальному процесі України: практика правозастосування. *Права людини в умовах воєнного стану в Україні: Х круглий стіл до Всеукраїнського тижня права (10 грудня 2024 року). Права людини в умовах воєнного стану в Україні: до тижня права і Загальної декларації прав людини* : зб. наук. праць за матер. круглого столу, Київ, 10 грудня 2024 р. / редкол.: А.Ю. Нашинець-Наумова, Г.П. Цимбал, С.В. Бобровник, Т.О. Дідич, О.І. Чаплук, А.П. Чернега. Київ : Київ. столич. ун-т ім. Б. Грінченка, 2025. С. 63–67. URL: https://www.researchgate.net/publication/396154856_Kalanca_IG_Materialna_forma_isnuvanna_ak_vlastivist_dokazu_v_kriminalnomu_procesi_Ukraini_praktika_pravozastosuvanna_Prava_ludini_v_umovah_voennogo_stanu_v_Ukraini_X_kruglij_stil_do_Vseukrainskogo_tiz.

12. Каланча І. Г. Результати OSINT як джерело доказів у кримінальному процесі України. *Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій*: матеріали Всеукр. наук.-практ. конф. (м. Чернівці, 20 грудня 2024 р.) / відп. ред. К.А. Возняковська. ТОМ 1, Чернівці, 2024. С. 43–49. URL: https://www.researchgate.net/publication/389647938_Kalanca_IG_Rezultati_OSINT_a_k_dzerelo_dokaziv_u_kriminalnomu_procesi_Ukraini_Innovacii_vikliki_ta_novi_gorizonti_pravovogo_reguluvanna_u_svitli_sucasnih_socialno-ekonomichnih_ta_politicnih_transformaci.

13. Каланча І. Г. Використання висновку експерта, що має електронну форму як доказу в кримінальному процесі України. *Актуальні проблеми національного законодавства*: збірник матеріалів Міжнародної науково-практичної конференції, м. Кропивницький, 17 квітня 2025 року. Частина 1. Кропивницький, 2025. С. 154–156. URL:

https://www.researchgate.net/publication/392901845_Kalanca_IG_Vikoristanna_visnovku_eksperta_so_mae_elektronnu_formu_ak_dokazu_v_kriminalnomu_procesi_Ukraini_Aktualni_problemi_nacionalnogo_zakonodavstva_zbirnik_materialiv_Miznarodnoi_na_ukovo-practicno.

14. Каланча І. Термінологічне розмежування понять «електронний доказ», «цифровий доказ» і «доказ, що має електронну форму» в кримінальному процесі України. *Пріоритетні шляхи розвитку науки і освіти*: матеріали XV Міжнародної науково-практичної конференції (м. Львів, 9–10 травня 2025 року). Львів : Львівський науковий форум, 2025. С. 195-197. URL: <http://www.lviv-forum.inf.ua/save/2025/9-10.05/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA.pdf>.

15. Власова Г. П., Каланча І. Г. Захисник як суб'єкт роботи з електронними доказами в кримінальному провадженні. *Актуальні питання реформування правової системи* : зб. матеріалів XXII Міжнар. наук.-практ. конф., Луцьк, 13-15 червня 2025 р. / Уклад. Джурак Л. М. Луцьк : Вежа-Друк, 2025. С. 113–115. URL: https://www.law.vnu.edu.ua/files/ugd/65dd18_5ab2de833d004115b0483aa2420d7cc0.pdf.

Праці, які додатково відображають результати дослідження:

1. Каланча І. Г. Організація навчання представників органів кримінальної юстиції сучасним процесуально-цифровим компетентностям. Training legal professionals following European standards: scientific and pedagogical internship, November 4 – December 15, 2024. Riga, the Republic of Latvia. p.p. 45-50.

2. Каланча І. Г., Щербанюк О. В. Досудовий процес. Навчально-методичний посібник. Чернівці: Рута. Чернівецький національний університет імені Юрія Федьковича, 2020. 200 с.

3. Шевчук П. В., Каланча І. Г. Кримінальний процес : навчально-методичний посібник для здобувачів вищої освіти першого (бакалаврського) рівня; галузь знань – 08 «Право»; спеціальність – 081 «Право». Чернівці, 2024. 184 с.

ANNOTATION

Kalanča I. H. Evidence in electronic form in criminal procedure of Ukraine: theory and practice. – Qualification scientific work in the form of a manuscript.

Dissertation for the Degree of Doctor of Law in the Specialization 12.00.09 – criminal process and forensics; forensic examination; operational and investigative activities. – National Academy of Internal Affairs, Kyiv, 2025.

The present study employs a doctrinal approach to substantiate the conceptual foundations of the institution of evidence in electronic form in the criminal procedure of Ukraine. In this regard, the study determines the procedural nature of the aforementioned institution, as well as the peculiarities of its sources of origin. Furthermore, the study determines the procedure for its identification, collection, acquisition, procedural recording, storage, and use. In addition to the aforementioned, the study develops organisational and practical approaches to improving the criminal procedural regulation of the activities of criminal proceedings subjects in working with such evidence in the context of global digitalisation.

It has been demonstrated that the electronic component of criminal proceedings in Ukraine consists of five elements: electronic criminal proceedings; digitisation of criminal proceedings materials and their backup storage; evidence in electronic form; electronic devices for evidential purposes; and electronic tools for the exercise of powers by law enforcement agencies.

It has been argued that "digital evidence" corresponds to the content of the evidence, "electronic evidence" corresponds to the technical means of its implementation, and "evidence in electronic form" corresponds to the procedural form of presentation.

The establishment of the institution of evidence in electronic form in the Ukrainian criminal process is contingent on two factors. Firstly, technological developments have increased the volume of electronic data in criminal proceedings. Secondly, the internal need of criminal procedural science to highlight its own vision of the new digital reality has been identified. The establishment of the relevant institution is characterised by

competition between doctrinal approaches (ranging from identification with documents or material evidence to proposals to distinguish them as an independent procedural source of evidence) and significant terminological variability. Notwithstanding the extensive theoretical foundation that has been established through the endeavours of domestic scholars, there is an imperative to re-evaluate them as an autonomous institution.

It has been proven that the procedural nature of evidence in electronic form in criminal proceedings lies in the possibility of its potential belonging to all procedural sources of evidence specified in Article 84 of the Ukrainian Criminal Procedure Code. The fact that the evidence under scrutiny belongs to a particular procedural source determines the procedural order of its handling during criminal proceedings. Consequently, this also establishes the criteria for assessing its admissibility.

The technical nature of evidence in electronic form is determined by a set of characteristics of the information environment in which it is created and stored, as well as by the properties of electronic media that are examined during criminal proceedings. Evidence in electronic form functions as a four-level structure: content, metadata, system shell, and electronic information carrier, which has a material expression. The technical aspects of evidence in the category under study are highlighted, including metadata; the distinction between logical copying and bit-by-bit copying; hashing; electronic signatures; and electronic time stamps. The process of hashing serves to verify the identity of a digital object and to detect any alterations, thereby establishing a technical foundation for confirming the integrity and immutability of computer data.

A set of algorithms has been developed, which is proposed as three strategies for securing evidence in electronic form in criminal proceedings in Ukraine: physical seizure of electronic media or computer systems; inspection and copying of computer data; inspection and recording of information from open sources.

The mechanisms employed to achieve this objective are organised in accordance with the degree of reliability and defined as follows:

- packaging and labelling of electronic media;
- recording of general and unique hardware identifiers;
- description of the structure and content of computer data and their metadata;

- hashing of computer data and sequential recording of computer data checksums in procedural documents; and

- use of qualified electronic signatures and electronic time stamps. A systematic study of the concept of chain of custody and its organisational and technical models has demonstrated the need for further research and the prospect of institutionalisation.

The effectiveness of evidence management in electronic form within the Ukrainian criminal justice system is contingent upon the organisational capacity of the institutions responsible for its implementation. The organisational readiness of criminal proceedings participants to work with evidence in electronic form should be considered through three interrelated components: material and technical; personnel; and regulatory.

The procedural powers and functional roles of subjects of criminal proceedings in interaction with evidence in electronic form have been systematically studied, including the investigator, prosecutor, defence attorney, investigating judge and court, expert, and specialist.

The role of the investigator in working with evidence in electronic form has been determined to be system-forming. The efficacy of such activities is contingent upon a synthesis of legal aptitude and foundational digital literacy. This encompasses an appreciation of the intricacies of computer data and metadata, logical protection mechanisms, hashing algorithms, and the distinctions between logical and bitwise copying. Additionally, proficiency in OSINT tools is imperative for the expeditious identification of pertinent traces.

The prosecutor in criminal proceedings is a key figure in ensuring the proper handling of evidence in electronic form, coordinating the actions of the investigator, operational units, specialists, and experts, and monitoring compliance with the criteria of relevance, admissibility, and reliability. The responsibilities of the aforementioned parties include the lawful selection of the method of obtaining information (copying information or seizing the information carrier), the recording of identification parameters of computer data (in particular, hash values) in protocols, the verification of the authenticity of electronic documents and electronic signatures, the organisation of the disclosure of pre-

trial investigation materials to the defence in accordance with Article 290 of the CPC of Ukraine, and the use of mechanisms of international cooperation.

The defense attorney in criminal proceedings acts as an independent subject of evidentiary activity with regard to evidence in electronic form, exercising the right to use it guaranteed by Part 2 of Article 22 and Part 3 of Article 93 of the Criminal Procedure Code of Ukraine. The effectiveness of this activity is determined by a combination of procedural activity and technical ability to ensure the authenticity and integrity of digital data (in accordance with DSTU ISO/IEC 27037:2017). In the context of the search and disclosure of materials to the other party (Article 290 of the CPC of Ukraine), the following priorities are identified: the minimisation of interference in private life, the protection of attorney-client privilege, the requirement of the provision of forensic (household) copies and control identifiers, and procedural responses to procedural violations.

The investigating judge and the court form a single framework for procedural control over evidence in electronic form: the former through prior authorisation of interference in the digital environment and the determination of restrictions on digital devices, the latter through the examination of evidence in electronic form and verification of its relevance, admissibility, reliability, and sufficiency.

The procedural role of the expert is centred on scientifically verified research, the utilisation of certified methods, and the formulation of expert conclusions. The specialist performs the technical function of DEFR: identification, fixation, preservation, and initial analysis of digital traces in accordance with DSTU ISO/IEC 27037:2017, with procedural recording of their participation and results. The necessity for a distinct allocation of competencies among the subjects of criminal proceedings is emphasised.

The Berkeley Protocol is regarded as a comprehensive methodology for working with data from open sources, combining legal, ethical, and technical standards (identification of sources, proper collection, preservation, verification, documentation of the chain of custody). In the context of Ukrainian criminal proceedings, the implementation of this system is expected to enhance the evidentiary quality of OSINT materials, mitigate the risks of inadmissibility, and satisfy the security requirements of

the participants in the proceedings. Concurrently, the discrepancy between the literal utilisation of the term "Berkeley Protocol" and its practical compliance, in conjunction with the absence of a consolidated procedure for handling open source data within the CPC of Ukraine, underscores the imperative for regulatory elucidation.

It has been proven that the Convention on Cybercrime defines a procedural model for inter-state cooperation on working with evidence in electronic form. These instruments have been partially implemented in the CPC of Ukraine, but key gaps remain. The Second Additional Protocol has been shown to deepen cooperation (through direct appeals to providers, expedited procedures, emergency provisions, and data protection standards) and to set the vector for improving the CPC of Ukraine.

It is therefore reasonable that ISO/IEC 27037:2012, which has been integrated into European legislation as EN ISO/IEC 27037:2016 and implemented in Ukraine through DSTU ISO/IEC 27037:2017, forms the methodological core of handling evidence in electronic form. This includes its identification, collection, acquisition (image creation), and preservation with integrity, reproducibility, and verifiability. Notwithstanding the existence of the aforementioned DSTU, the prevailing regulatory framework in Ukraine, namely the Criminal Procedure Code, exhibits a lacuna in terms of the separation of the processes of identification, collection, and acquisition of evidence in electronic form, the procedural consolidation of the roles of DEFR and DES, the recording of the chain of custody, and so forth.

A comparative analysis of foreign experience demonstrates that evidence in electronic form has become a systemic element of criminal proceedings. The effectiveness of its use is determined by a combination of clear procedural frameworks, institutional capacity, and transnational cooperation.

It has been proven that improving the organizational basis for working with evidence in electronic form is an important factor in adapting Ukraine's criminal process to the digital age. The effectiveness of this direction is determined by the level of material and technical support for criminal proceedings, the availability of qualified personnel, and the capacity for interagency cooperation. The training of specialised personnel, the establishment of forensic IT laboratories, and the introduction of interdisciplinary training

programmes form the basis of the institutional capacity of the criminal justice system. The standardisation of criminal proceedings through the development of standard operating procedures ensures uniformity of practice, predictability of actions, and reduces the risk of evidence loss.

A coordinated approach to procedural improvements in the handling of evidence in electronic form is proposed, involving the development of a regulatory framework that maintains a balance between legal certainty and technical adaptability, prevents excessive formalisation of procedures, and at the same time guarantees the authenticity, integrity, and admissibility of evidence in this category. The proposed amendments to the CPC of Ukraine provide for the phased implementation of the Convention on Cybercrime and European acts. The phased introduction of the relevant provisions should be accompanied by training for criminal justice actors, the formalisation of standard operating procedures, and the creation of mechanisms for interagency coordination.

The necessity for technical enhancement in the management of evidence in electronic form has been substantiated, with the objective being the effective utilisation of such evidence. This necessitates the establishment of an infrastructure that incorporates certified identification and storage systems.

A concept for improving the institution of evidence in electronic form in the criminal process in Ukraine has been developed, aimed at creating a unified, scientifically sound, and technologically integrated mechanism for its procedural circulation. The fundamental principle underpinning this approach is the comprehensive development of a range of disciplines, including regulatory, organisational, infrastructural, technical-criminalistic, educational, and scientific-analytical domains.

Keywords: criminal proceedings, evidence in electronic form, ISO/IEC 27037:2012, identification, acquisition, hashing, integrity, Berkeley Protocol, Convention on Cybercrime, cybersecurity, digital technologies, databases, standard operating procedures, electronic evidence, digital evidence.

ЗМІСТ

АНОТАЦІЯ	2
ЗМІСТ	22
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	25
ВСТУП	27
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ДОКАЗІВ ЕЛЕКТРОННОЇ ФОРМИ У КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ	46
1.1. Вітчизняні доктринальні підходи до розуміння доказів та їх властивостей у кримінальному процесі України	46
1.2. Концептуальні підходи до доказів електронної форми у кримінальному процесі України	71
1.3. Ретроспектива формування інституту електронних (цифрових) доказів у кримінальному процесі України	91
1.4. Процесуальна та технічна природа доказів електронної форми у кримінальному процесі України	108
РОЗДІЛ 2. ПРАКТИКА РОБОТИ З ДОКАЗАМИ ЕЛЕКТРОННОЇ ФОРМИ У КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ	156
2.1. Практика пошуку та фіксації доказів електронної форми у кримінальному процесі України	156
2.2. Механізми підтвердження цілісності та автентичності доказів електронної форми в кримінальному провадженні	176
2.3. Організаційні аспекти роботи з доказами електронної форми у кримінальному процесі України	194
РОЗДІЛ 3. ПРОЦЕСУАЛЬНІ ПОВНОВАЖЕННЯ ТА ФУНКЦІОНАЛЬНІ РОЛІ СУБ'ЄКТІВ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ У ВЗАЄМОДІЇ З ДОКАЗАМИ ЕЛЕКТРОННОЇ ФОРМИ	211

3.1. Слідчий як суб'єкт роботи з доказами електронної форми в кримінальному провадженні	211
3.2. Прокурор як суб'єкт роботи з доказами електронної форми в кримінальному провадженні	227
3.3. Захисник як суб'єкт роботи з доказами електронної форми в кримінальному провадженні	238
3.4. Суддя та слідчий суддя як суб'єкти роботи з доказами електронної форми в кримінальному провадженні	253
3.5. Інші учасники кримінального провадження як суб'єкти роботи з доказами електронної форми в кримінальному провадженні	273

РОЗДІЛ 4. МІЖНАРОДНІ ПРОЦЕДУРИ ПОШУКУ, ФІКСАЦІЇ ТА ВИКОРИСТАННЯ ДОКАЗІВ ЕЛЕКТРОННОЇ ФОРМИ

290

4.1. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних (Berkeley Protocol on Digital Open Source Investigations) та застосування його вимог під час кримінального провадження	290
4.2. Механізми Конвенції про кіберзлочинність та практика їх застосування в кримінальному процесі України	302
4.3. Практика впровадження стандарту ISO/IEC 27037:2012 в державах Європи та в Україні	320
4.4. Зарубіжний досвід роботи з доказами електронної форми в кримінальному процесі	330

РОЗДІЛ 5. ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ РОБОТИ З ДОКАЗАМИ ЕЛЕКТРОННОЇ ФОРМИ У КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ

351

5.1. Організаційні аспекти вдосконалення роботи з доказами електронної форми у кримінальному процесі України	351

5.2. Шляхи вдосконалення процесуального регулювання використання доказів електронної форми у кримінальному процесі України	371
5.3. Напрями технічного удосконалення використання доказів електронної форми у кримінальному процесі України	394
5.4. Концепція вдосконалення інституту доказів електронної форми у кримінальному процесі України	409
ВИСНОВКИ	422
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	434
ДОДАТКИ	501

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВР України – Верховна Рада України

ВС – Верховний Суд

ГПК України – Господарський процесуальний кодекс України

Другий додатковий протокол – Другий додатковий протокол до Конвенції про кіберзлочинність щодо посилення співпраці та розкриття доказів електронної форми від 23.11.2021 (підписаний 30.11.2022, не ратифікований)

ДСТУ ISO/IEC 27037:2017 – ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів»

ЕІС, КС, МТСЗ – електронні інформаційні системи, комп'ютерних систем або їх частини, мобільні термінали систем зв'язку

ЕНІ – електронні носії інформації

ЄРДР – Єдиний реєстр досудових розслідувань

ЄС – Європейський Союз

ЄСПЛ – Європейський суд з прав людини

Закон України «Про електронні документи та електронний документообіг» – Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV

Закон України «Про електронну ідентифікацію та електронні довірчі послуги» – Закон України «Про електронну ідентифікацію та електронні довірчі послуги» від 5 жовтня 2017 року № 2155-VIII

інформація, що міститься в ІС – інформація, міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах

ІС – інформаційна система

ІТ – інформаційні технології

КАС України – Кодекс адміністративного судочинства України

КЕП – кваліфікований електронний підпис

КЗПЛ – Конвенція про захист прав людини і основоположних свобод, ратифікована Законом України від 17.07.1997 № 475/97-ВР

КК України – Кримінальний кодекс України

ККС – Касаційний кримінальний суд

Конвенція про кіберзлочинність – Конвенція про кіберзлочинність від 23.11.2001, ратифікована Законом України від 07.09.2005 № 2824-IV

КПК – Кримінально-процесуальний кодекс

КПК України – Кримінальний процесуальний кодекс України

МВС України – Міністерство внутрішніх справ України

НАБУ – Національне антикорупційне бюро України

НКП 24/7 – національний контактний пункт, що забезпечує цілодобову взаємодію з іншими державами в межах процедур Конвенції про кіберзлочинність

НПА – нормативно-правовий акт

НСРД – негласні слідчі (розшукові) дії

ОГП – Офіс Генерального прокурора

ПЗ – програмне забезпечення

Протокол Берклі – Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних (Berkeley Protocol on Digital Open Source Investigations)

СБУ – Служба безпеки України

СОП – стандартні операційні процедури

ЦПК України – Цивільний процесуальний кодекс України

DEFR (Digital Evidence First Responders) – фахівець, що здійснює первинну взаємодію з доказом електронної форми

DES (Digital Evidence Specialist) – фахівець з цифрової криміналістики

e-Case – електронна система управління кримінальними провадженнями щодо корупційних правопорушень e-Case Management System

ISO/IEC 27037:2012 – ISO/IEC 27037:2012 «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence»

OSINT (Open Source Intelligence) – розвідка на основі відкритих джерел

ВСТУП

Актуальність теми. Глибокі трансформації, що відбуваються під впливом цифровізації суспільних відносин, зумовлюють докорінне переосмислення доктрини кримінального процесуального доказування. Сьогодні чимало інформації, що може мати доказове значення у кримінальному провадженні, існує в електронній формі – у вигляді цифрових даних, записів комунікацій, інформації з технічних пристроїв, мережевих ресурсів та електронних систем. Зазначене об'єктивно висуває перед правовою наукою і практикою завдання формування нового концептуального підходу до розуміння, класифікації та використання доказів електронної форми під час кримінального провадження.

На відміну від традиційних матеріальних джерел доказової інформації, електронні дані характеризуються нестабільністю, можливістю несанкціонованої модифікації, складністю перевірки їх автентичності та цілісності, ризиком випадкової втрати. Вони водночас є носіями як змістовної, так і технічної інформації, що спричиняє необхідність поєднання правових, криміналістичних та інформаційно-технологічних підходів до їх аналізу. Ось чому проблеми визначення процесуальної природи доказів електронної форми, порядку їх фіксації, зберігання, перевірки та процесуальної оцінки набувають стратегічного значення для забезпечення законності й ефективності кримінального провадження.

У чинному кримінальному процесуальному законодавстві України досі бракує чіткої регламентації процедури обігу доказів електронної форми, а це породжує неоднакове їх розуміння та застосування в практиці органів досудового розслідування, прокуратури й суду.

Теоретичною базою дисертаційного дослідження є праці у сфері доказів та доказування таких вітчизняних науковців як О. В. Баганець, В. В. Вапнярчук, В. П. Гмирко, Ю. М. Грошевий, О. В. Капліна, Є. Г. Коваленко, С. О. Ковальчук, Г. Р. Крет, М. М. Михеєнко, В. Т. Нор, М. А. Погорецький, Д. Б. Сергєєва, В. А. Смирнов, О. С. Старенький, С. М. Стахівський, В. Я. Тацій, О. Г. Шило, М. Є. Шумило, О. Г. Яновська а також роботи інших вчених-процесуалістів.

У сфері вітчизняного кримінального процесу загальнотеоретичні питання доказів електронної форми досліджували Д. О. Алексєєва-Процюк, М. В. Багрій, О. М. Брисковська, Г. П. Власова, С. І. Гонгало, М. І. Демура, О. В. Капліна, А. В. Коваленко, С. О. Ковальчук, О. Г. Козицька, Д. І. Клепка, В. В. Мурадов, М. А. Погорецький, Д. Б. Сергєєва, О. В. Сіренко, А. В. Скрипник, І. А. Смаль, О. С. Старенький, А. В. Столітній, В. М. Тertiшник, Л. Д. Удалова, Т. Г. Фоміна, В. Г. Хахановський, Є. С. Хижняк та інші. Відомі прикладні розробки таких науковців, як А. О. Антощук, Н. М. Ахтирська, І. В. Гловюк, І. В. Гора, А. В. Гутник (Ратнова), В. А. Колесник, І. О. Крицька, О. П. Метелев, Д. І. Овсянюк, Ю. Ю. Орлов, М. І. Пашковський, І. А. Тітко, О. О. Торбас, Д. М. Цехан, С. С. Чернявський та інші.

Особливу актуальність тема набуває у контексті імплементації міжнародних стандартів у сферу доказів електронної форми. Конвенція про кіберзлочинність та Другий додатковий протокол до неї закріплюють основи міжнародного співробітництва у сфері збирання й передання доказів електронної форми. Європейський Союз у 2023 році ухвалив низку нормативно-правових актів, що визначають уніфіковані підходи до надання, збереження та збору доказів електронної форми під час кримінального провадження. Для України, яка прагне інтегруватися у єдиний європейський простір, адаптація цих положень є не лише науково, а й політично важливою.

Сучасні виклики – зокрема, воєнний стан, зростання кіберзлочинності, масове використання інформаційно-комунікаційних технологій у публічній і приватній сферах – вимагають побудови цілісної системи правового регулювання доказів електронної форми у кримінальному процесі України. У цьому контексті наукове осмислення правової природи таких доказів, формулювання їх доктринального обґрунтування, визначення критеріїв автентичності та цілісності, а також розроблення ефективних процесуальних і технічних механізмів роботи з ними набуває першорядного значення для подальшого розвитку кримінальної процесуальної науки та вдосконалення національного законодавства.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до абз. 11, 13, 15 розділу «Протидія злочинності» Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року, схваленої розпорядженням Кабінету Міністрів України від 15 листопада 2017 р. № 1023-р; § 4 Розділу 4 Національної стратегії у сфері прав людини, затвердженої Указом Президента України від 24 березня 2021 р. № 119/2021; п. 4.1.4 Розділу I Стратегії розвитку системи правосуддя та конституційного судочинства на 2021–2023 рр., затвердженої Указом Президента України від 11 червня 2021 р. № 231/2021; цілей С. 2 та С. 3 розділів 5 та 6 Стратегії кібербезпеки України, схваленої рішенням Ради національної безпеки і оборони України від 14 травня 2021 р. та уведеної в дію Указом Президента України від 26 серпня 2021 р. № 447/2021; п.п. 10, 16, 26 Плану реалізації Стратегії кібербезпеки України, схваленого рішенням Ради національної безпеки і оборони України від 30 грудня 2021 р. та уведеного в дію Указом Президента України від 1 лютого 2022 р. № 37/2022; п.п. 5.1–5.9 Розділу II Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 рр., схваленого Указом Президента України від 11 травня 2023 р. № 273/2023; розділу «Інформаційні та комунікаційні технології» Переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні, затвердженого постановою Кабінету Міністрів України від 30 квітня 2024 р. № 476; п.п. 2.7, 3.1.1, 3.1.2, 3.2, 3.3, 3.3.1–3.3.4, 4.5, 4.6 Стратегії розвитку прокуратури на 2025–2028 рр., затвердженої наказом Генерального прокурора № 322 від 8 жовтня 2025 р.

Тему дисертації затверджено рішенням Вченої ради Національної академії внутрішніх справ 24 червня 2025 року (протокол № 16/4-3).

Мета і задачі дослідження. Метою дисертації є теоретико-правове узагальнення та розв'язання комплексної наукової і прикладної проблеми формування цілісної концепції доказів електронної форми у кримінальному процесі України.

Для досягнення зазначеної мети поставлено такі *задачі*:

- дослідити вітчизняні доктринальні підходи до розуміння доказів та їх властивостей у кримінальному процесі України в контексті формування науково-теоретичної основи для доказів електронної форми;
- сформулювати теоретико-методологічні засади дослідження доказів електронної форми як складової кримінального процесу України;
- дослідити історичний розвиток теоретичних підходів до доказів електронної форми у кримінальному процесі України;
- визначити місце доказів електронної форми в системі процесуальних джерел доказів у кримінальних провадженнях, охарактеризувати їх процесуальну та технічну природу;
- запропонувати алгоритми пошуку та фіксації доказів електронної форми в кримінальному процесі України;
- розробити методику підтвердження автентичності та цілісності доказів електронної форми в кримінальному процесі України;
- систематизувати підходи до організації роботи з доказами електронної форми в системі органів кримінальної юстиції України;
- визначити й деталізувати повноваження слідчого як суб'єкта роботи з доказами електронної форми у кримінальному провадженні;
- охарактеризувати особливості процесуальної діяльності прокурора щодо збирання та оцінки доказів електронної форми у кримінальному провадженні;
- охарактеризувати специфіку діяльності захисника при роботі з доказами електронної форми у кримінальному провадженні;
- установити процесуальні повноваження судді та слідчого судді при дослідженні доказів електронної форми у кримінальному провадженні;
- охарактеризувати особливості участі інших учасників кримінального провадження при роботі з доказами електронної форми: експерта, спеціаліста в сфері цифрової криміналістики, спеціаліста в сфері OSINT;
- сформулювати пропозиції щодо використання Протоколу Берклі з ведення розслідувань з використанням відкритих цифрових даних (Berkeley Protocol on

Digital Open Source Investigations) як методологічної основи фіксації інформації з відкритих джерел під час кримінального провадження;

- визначити особливості процесуальних механізмів, визначених Конвенцією про кіберзлочинність щодо роботи з доказами електронної форми у кримінальному провадженні;

- розкрити специфіку ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» як методологічної складової щодо роботи з доказами електронної форми під час кримінального провадження;

- узагальнити зарубіжний досвід роботи з доказами електронної форми та міжнародну практику використання електронних інформаційних систем для міжнародного обміну доказами під час кримінального провадження;

- виокремити засади організації роботи з доказами електронної форми у кримінальному процесі України;

- розкрити процесуальні аспекти роботи з доказами електронної форми у кримінальному процесі України;

- підготувати пропозиції щодо вдосконалення технічних аспектів роботи з доказами електронної форми у кримінальному процесі України;

- сформулювати концептуальне бачення щодо подальшого удосконалення інституту доказів електронної форми у кримінальному процесі України.

Об'єкт дослідження – суспільні відносини, що виникають у процесі кримінального провадження під час пошуку, фіксації, перевірки, оцінки та використання доказів електронної форми, а також механізми їх процесуального обігу в системі кримінальної юстиції України.

Предмет дослідження – докази електронної форми у кримінальному процесі України.

Методи дослідження. Для досягнення поставленої мети та вирішення обумовлених нею задач використовувались такі методи:

- *діалектичний* – для з'ясування сутності, змісту та закономірностей розвитку доказів електронної форми у кримінальному процесі в динаміці

становлення інформаційного суспільства та цифровізації кримінальної юстиції (розділи 1, 2, 5); його застосування дозволило визначити внутрішні суперечності між технічною природою електронних даних і традиційними процесуальними механізмами доказування;

– *системний аналіз* – сприяв аналізу взаємодії процесуальних, організаційних та технічних складників механізму роботи з доказами електронної форми, що дозволило сформувати концептуальну модель їх процесуального статусу та обігу (розділи 1–5);

– *структурно-функціональний* – для виявлення взаємозв'язку елементів системи процесуального регулювання доказів електронної форми, їх місця у системі процесуальних джерел доказів, а також для розмежування понять і категорій (розділи 1–3);

– *історико-правовий* – для дослідження етапів формування уявлень про докази електронної форми (підрозділ 1.1 та 1.3), генези становлення та розвитку нормативних підходів до їх використання у кримінальному процесі, починаючи від перших спроб легалізації цифрових даних до сучасного етапу впровадження електронних систем правосуддя (розділи 1, 2);

– *компаративістський* – дав змогу здійснити порівняльний аналіз зарубіжного досвіду регламентації доказів електронної форми, насамперед у контексті імплементації положень Конвенції про кіберзлочинність, Другого додаткового протоколу до неї та законодавства Європейського Союзу в національну правову систему (розділ 4);

– *логіко-юридичний* – для формулювання авторських дефініцій ключових понять і для обґрунтування пропозицій щодо вдосконалення їх процесуального регулювання (розділи 1–3, 5);

– *формально-юридичний* – для аналізу норм чинного КПК України, законів України та підзаконних нормативно-правових актів, практики їх застосування органами досудового розслідування, прокуратури та суду (розділи 2–5);

– *моделювання* – дозволив розробити пропозиції щодо вдосконалення роботи з доказами електронної форми у кримінальному процесі України (розділ 5);

– *статистичний* – під час аналізу результатів емпіричного дослідження, що включало узагальнення практики органів досудового розслідування, судів, прокуратури та адвокатури щодо роботи з доказами електронної форми (розділи 2–3);

– *соціологічний* – для отримання емпіричних даних про стан застосування доказів електронної форми у кримінальному провадженні, рівень цифрової компетентності слідчих, прокурорів, суддів і адвокатів, а також для виявлення проблем правозастосування (розділи 2-4).

Дослідження ґрунтується на інтеграції кримінальної процесуальної теорії доказів з положеннями цифрової криміналістики, правової інформатики та кібербезпеки. Це забезпечило комплексне розкриття правової природи доказів електронної форми з формуванням нових теоретико-методологічних положень щодо їх ідентифікації, збирання, зберігання, перевірки та оцінки в умовах цифровізації правосуддя.

Емпіричну базу дослідження становлять: зведені дані вивчення 350 кримінальних проваджень упродовж 2018–2025 рр.; 450 ухвал, постанов та вироків судів України усіх регіонів; 30 рішень Європейського суду з прав людини; результати опитування 1301 респондента, серед яких: 128 суддів, 574 прокурори, 100 адвокатів, 146 слідчих та детективів, 174 співробітники оперативних підрозділів, 59 судових експертів та ІТ-фахівців, що виконують функції спеціалістів під час кримінального провадження, 120 науковців; статистичні та аналітичні звіти й узагальнення Верховного Суду, Національної поліції України, Офісу Генерального прокурора, Ради Європи.

Наукова новизна одержаних результатів полягає в тому, що дисертація є першим в Україні комплексним дисертаційним дослідженням, в якому реалізовано доктринальний підхід до формування цілісної концепції доказів електронної форми у кримінальному процесі України з визначенням шляхів розв’язання низки фундаментальних і праксеологічних проблем удосконалення правових, організаційних, процедурних і технічних засад їх формування, перевірки, оцінювання та використання. Найсуттєвішими з них є такі положення:

вперше:

– запропоновано цілісне бачення електронної складової кримінального процесу України, що містить п'ять елементів: електронне кримінальне провадження; оцифрування матеріалів кримінальних проваджень та їх резервне зберігання; докази електронної форми; електронні інструменти доказування; електронні інструменти реалізації повноважень суб'єктів правозастосування. Обґрунтовано інституційну самостійність доказів електронної форми у кримінальному процесі України, що обумовлює формування їх належної теоретичної та нормативної основи. У цьому напрямі розмежовано понятійний апарат в межах ключових для практики правозастосування категорій: «джерело доказів», «документ», «електронний документ», «носії інформації», «комп'ютерні дані» тощо. Дано визначення понять «електронні докази», «докази електронної форми» та «цифрові докази» і обґрунтовано підхід до використання термінів, за якого «цифровий доказ» відповідає змісту доказу, «електронний доказ» – технічному способу його реалізації, а «доказ електронної форми» – процесуальній формі подання;

– сформульовано комплекс алгоритмів пошуку та фіксації доказів електронної форми, що об'єднаний за трьома функціонально-структурними категоріями і виступає як три самостійні стратегії фіксації доказів електронної форми у кримінальному процесі України: 1) фізичне вилучення електронних носіїв інформації або комп'ютерних систем; 2) огляд та копіювання комп'ютерних даних; 3) огляд та фіксація інформації з відкритих джерел. Запропонований підхід (у межах перших двох стратегій) визначає пріоритет огляду та копіювання комп'ютерних даних, здійснених з дотриманням вимог ч. 4 ст. 99 КПК України (за участю спеціаліста) та норм ДСТУ ISO/IEC 27037:2017, процесуально та технологічно допустимою альтернативою фізичному вилученню технічних пристроїв, здатною забезпечити завдання доказування. Запропоновано алгоритм здобуття високоінформативних доказів електронної форми, що поєднує національні та міжнародні процедури й передбачає: 1) фіксацію відомостей з відкритих джерел у порядку ч. 4 ст. 99, ст. 237 або ст. 240 КПК України (фіксація

публічно доступних даних); 2) скерування запиту про термінове збереження комп'ютерних даних в порядку ст.ст. 16, 29 або 17, 30 Конвенції про кіберзлочинність (зберігання даних та отримання оперативної інформації щодо публічно недоступного сегменту відомостей); 3) скерування запиту про міжнародну правову допомогу в порядку ст. 551 КПК України для отримання даних, збережених відповідно до механізмів Конвенції про кіберзлочинність (отримання повних відомостей від держателя даних, що є процесуально допустимими доказами);

– обґрунтовано методику підтвердження автентичності та цілісності доказів електронної форми в кримінальному процесі України, засновану на техніко-криміналістичних (ДСТУ ISO/IEC 27037:2017) інструментах ідентифікації комп'ютерних даних і процесуальних (абз. 3 п. 3 ч. 3 ст. 104 КПК України) вимогах послідовної фіксації й перевірки таких ідентифікаторів, контролю доступу та забезпечення безпеки доказів. У межах відповідної методики запропоновано багаторівневу систему, диференційовану за ступенем зростання рівня надійності методів, що включає: 1) упакування та маркування електронних носіїв інформації; 2) фіксацію загальних та унікальних апаратних ідентифікаторів; 3) опис структури і змісту комп'ютерних даних та їх метаданих; 4) гешування комп'ютерних даних і послідовної фіксації контрольних сум комп'ютерних даних у процесуальних документах; 5) фіксацію стану доказу електронної форми у визначений часовий період за допомогою КЕП з електронною позначкою часу; 6) фіксацію ланцюга збереження доказів (chain of custody) в порядку ДСТУ ISO/IEC 27037:2017. Обґрунтовано необхідність розроблення та впровадження стандартних операційних процедур (СОП) щодо роботи з доказами електронної форми, заснованих на ДСТУ ISO/IEC 27037:2017, ДСТУ ISO/IEC 27001:2023, ДСТУ ISO/IEC 27002:2023, закріплення практики фіксації ланцюга збереження доказів (chain of custody);

– сформульовано наукове бачення місця та ролі ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» як

методологічної основи технічного аспекту роботи з доказами електронної форми під час кримінального провадження на етапах їх ідентифікації, збирання, здобуття та збереження. Обґрунтовано необхідність його системного вивчення суб'єктами кримінального провадження, що здійснюють збирання та здобуття доказів електронної форми (впровадження процесуальної ролі Digital Evidence First Responder з релевантними вимогами до кваліфікації), впровадження в практику правозастосування та нормативну інституціоналізацію у відомчих нормативно-правових актах та стандартних операційних процедурах (СОП);

– сформульовано процесуальні аспекти вдосконалення роботи з доказами електронної форми у кримінальному процесі України: вдосконалення правового регулювання та імплементації положень Конвенції про кіберзлочинність; ДСТУ ISO/IEC 27037:2017 та Протоколу Берклі, що передбачає внесення системних змін до КПК України; зміни до законів України щодо зберігання інформації операторами телекомунікації, вимог до спеціалізації представників органів досудового розслідування, прокурорів та суддів, їх спеціалізації; прийняття міжвідомчого підзаконного нормативно-правового акту щодо взаємодії органів досудового розслідування та органів прокуратури з національним контактним пунктом 24/7; прийняття суб'єктами кримінального провадження відомчих актів щодо організації роботи з доказами досліджуваної категорії – стандартних операційних процедур (СОП);

– розроблено концептуальні підходи до вдосконалення інституту доказів електронної форми у кримінальному процесі України, що включають: 1. Загальні положення. 2. Нормативний напрям: оновлення термінології КПК України; автентичність і цілісність; розмежування збирання та здобуття; OSINT; термінове збереження й аналіз даних про рух інформації; захист приватності та обмеження втручання. 3. Організаційний напрям: ефективна взаємодія між суб'єктами кримінального провадження; системні рішення щодо посилення кадрового потенціалу; створення сталого каналу міжвідомчої співпраці з провайдерами телекомунікації. 4. Інфраструктурний напрям: створення інтегрованої системи управління доказами; побудова цифрової інфраструктури для обміну даними між

органами досудового розслідування, прокуратури та провайдерами телекомунікації, налагодження цифрової форми виконання ухвал про тимчасовий доступ до речей і документів. 5. Техніко-криміналістичний напрям: належне матеріально-технічне забезпечення органів досудового розслідування, прокуратури та суду; стандартизація форматів зберігання доказів електронної форми, методів ідентифікації, запровадження практики резервного копіювання, використання надійних електронних носіїв інформації, здатних забезпечити довготривале зберігання даних; криптографічне шифрування даних. 6. Освітній напрям: впровадження у вищих навчальних закладах юридичного та правоохоронного профілів компетентностей щодо роботи з доказами електронної форми; підвищення кваліфікації суб'єктів кримінального провадження; формування вимог щодо обов'язкових міждисциплінарних цифрових компетентностей. 7. Науково-аналітичний напрям: розширення та інституційна підтримка наукових досліджень за відповідною тематикою щодо вирішення актуальних практичних завдань та вдосконалення практики правозастосування; здійснення прикладних наукових досліджень; забезпечення систематичного моніторингу практики. 8. Очікувані результати та строки реалізації;

удосконалено:

– положення щодо місця доказів електронної форми в системі процесуальних джерел доказів у кримінальному процесі України, що полягає у можливості їх потенційної належності до всіх процесуальних джерел доказів, визначених ст. 84 КПК України. Обґрунтовано, що факт належності доказу досліджуваної категорії до певного процесуального джерела визначає процесуальний порядок поведінки з ними під час кримінального провадження та, як наслідок, критерії оцінки його допустимості. Електронна форма фіксації показань, у контексті ст. 225, ч. 11 ст. 615 КПК України, висуває додаткові вимоги до автентифікації допитуваної особи, збереження результатів технічної фіксації, підтвердження автентичності та цілісності. Обґрунтовано, що документами докази досліджуваної категорії визначаються через призму п. 1 та п. 3 ч. 2 ст. 99 КПК України, а також через призму електронних документів (у розумінні профільного закону), тоді як речові

докази репрезентовані фізичними об'єктами, наділення яких відповідним статусом обумовлене потребою встановлення належного правового режиму при їх вилученні та подальшим арештом. Висновок експерта електронної форми потребує обов'язкового підписання кваліфікованим електронним підписом, забезпечення належного процесуального способу отримання, підтвердження автентичності та відтворюваності змісту. Доказ електронної форми варто розглядати як чотирирівневу структуру, що містить контент, метадані, системну оболонку та електронний носій інформації, який має матеріальне вираження. Запропоновано класифікацію електронних носіїв інформації та обґрунтовано вплив відповідних характеристик на прийняття процесуальних рішень щодо пріоритизації фіксації нестабільних даних, вилучення технічних пристроїв, арешту майна тощо. Доведено, що гешування забезпечує відтворювану ідентифікацію цифрового об'єкта та виявлення будь-яких змін, слугуючи технічною основою для підтвердження цілісності та незмінності доказів електронної форми. Технічні характеристики доказів електронної форми, що здатні підтвердити автентичність та цілісність зафіксованих цифрових даних, в сукупності з застосовуваними належними кримінальними процесуальними процедурами, становлять дуалістичну основу процесуальної допустимості доказів електронної форми у кримінальному провадженні;

– процесуальні та організаційні повноваження слідчого як суб'єкта роботи з доказами електронної форми у кримінальному провадженні, що вимагають поєднання правових навичок із базовою цифровою грамотністю. Відповідні повноваження слідчого деталізовано в частині прийняття рішення щодо способу фіксації доказів електронної форми (здобуття – копіювання інформації чи збирання – вилучення носія інформації), вибору ідентифікаційних параметрів комп'ютерних даних та їх відображення у протоколах слідчих (розшукових) дій, залучення спеціаліста;

– процесуальні засади діяльності прокурора щодо роботи з доказами електронної форми у кримінальному провадженні як ключового суб'єкта, що поєднує координацію дій оперативних підрозділів, дізнавача, слідчого, залучення

спеціаліста, контроль за дотриманням критеріїв належності, допустимості й достовірності. Відповідні повноваження прокурора деталізовано в частині перевірки автентичності електронних документів і електронних підписів, організації відкриття матеріалів досудового розслідування стороні захисту відповідно до ст. 290 КПК України, використання механізмів міжнародної взаємодії, інтеграції доказів електронної форми у структуру обвинувачення, забезпечення підтвердження цілісності даних, джерела походження та зв'язку з юридично значущими обставинами. Запропоновано методологію оцінки процесуальних та технічних аспектів доказів електронної форми, на основі якої розроблено відповідні методичні документи;

– бачення процесуальної діяльності сторони захисту при роботі з доказами електронної форми у кримінальному провадженні як самостійного суб'єкта доказової діяльності щодо їх фіксації та представлення. Забезпечення ефективної реалізації останньої розглядається через поєднання процесуальної активності з технічною спроможністю підтвердити автентичність і цілісність комп'ютерних даних, дотримуючись стандарту доказування. Відповідні повноваження захисника деталізовано в контексті реалізації під час обшуку й доступу до матеріалів досудового розслідування (ст. 290 КПК України), щодо яких пріоритизовано мінімізацію втручання у приватне життя, охорону адвокатської таємниці, отримання доступу до криміналістичних (побітових) копій електронних носіїв інформації та їх ідентифікаторів, а також ефективне реагування на процесуальні порушення;

– наукове обґрунтування процесуальних повноважень та компетентностей судді та слідчого судді при дослідженні доказів електронної форми у кримінальному провадженні, що вимагає з'ясування відповідними суб'єктами низки техніко-правових критеріїв, серед яких: наявність у процесуальних документах геш-ідентифікаторів комп'ютерних даних і їх збіг з ідентифікаторами досліджуваних доказів, перевірюваність метаданих, електронних підписів і електронних позначок часу, відповідність процедур ідентифікації, збирання, здобуття та зберігання стандартам ДСТУ ISO/IEC 27037:2017; перевірка

автентичності матеріалів з відкритих джерел та процесуального порядку здобуття доказів електронної форми, одержаних в порядку міжнародної правової допомоги. Обґрунтовано необхідність надання переваги криміналістичним (побітовим) копіям як об'єктам аналізу, тоді як дослідження оригінального технічного пристрою допустиме лише за умов, що не створюють ризику цілісності доказу;

– наукові засади використання рекомендацій Протоколу Берклі з ведення розслідувань з використанням відкритих цифрових даних (Berkeley Protocol on Digital Open Source Investigations) як методологічної основи фіксації інформації з відкритих джерел під час кримінального провадження. Встановлено співвідношення положень п. 155 Протоколу Берклі з вимогами КПК України і запропоновано підхід до відображення відповідних відомостей в протоколі огляду кіберпростору;

– теоретико-прикладні засади реалізації процесуальних механізмів, визначених Конвенцією про кіберзлочинність щодо роботи з доказами електронної форми у кримінальному провадженні: 1) встановлення норм, що знайшли відображення в КПК України: поширення обшуку за межі комп'ютерної системи, яка є об'єктом первинного втручання (ч. 2 ст. 19 Конвенції) – абз. 2 ч. 6 ст. 236 КПК України; 2) норм, що не імplementовані, але які можуть бути реалізовані за допомогою існуючих процедур: термінове збереження комп'ютерних даних, які зберігаються (ст.ст. 16, 29), та порядок представлення (ст. 18) – частково через тимчасовий доступ до речей і документів (Глава 15 КПК України), перехоплення змісту даних, що передаються (ст. 21 Конвенції) – ст.ст. 263, 264 КПК України; 3) прогалин, що потребує внесення змін до КПК України: термінове збереження і часткове розкриття даних про рух інформації (ст.ст. 17, 30), збирання даних про рух інформації у режимі реального часу (ст. 20); добровільне надання інформації (ст. 26);

дістало подальший розвиток:

– дослідження вітчизняних доктринальних підходів до розуміння доказів та їх властивостей у кримінальному процесі України, реалізоване в контексті формування науково-теоретичної основи доказів електронної форми, де

електронна форма визначається характеристикою існування й подання фактичних даних у межах існуючих чотирьох видів (процесуальних джерел) доказів. Технологічний елемент і технічні характеристики доказів електронної форми визначено релевантними характеристиками, що впливають на такі властивості доказів як допустимість та достовірність;

– дослідження історичного розвитку теоретичних підходів щодо доказів електронної форми у кримінальному процесі України, яке засвідчило, що: становлення відповідного інституту характеризується конкуренцією доктринальних підходів (від ототожнення з документами чи речовими доказами до пропозицій їх виокремлення як самостійного процесуального джерела доказів) та значною термінологічною варіативністю; зумовлене технологічним розвитком, що збільшив обсяг електронних даних у кримінальних провадженнях, та внутрішньою потребою кримінальної процесуальної науки висвітлити власне бачення нової цифрової реальності. Обґрунтовано доцільність стриманого підходу щодо нормативного регулювання доказів електронної форми (без визнання самостійним процесуальним джерелом) та потреби застосування комплексного та технологічно орієнтованого підходу, що не дестабілізує систему кримінальної юстиції;

– узгоджені підходи до організації роботи з доказами електронної форми в системі органів кримінальної юстиції України через призму організаційної готовності суб'єктів кримінального провадження як три взаємопов'язані компоненти: 1) матеріально-технічний – забезпечення цифровими криміналістичними інструментами та інфраструктурою, сумісною з ДСТУ ISO/IEC 27037:2017; 2) кадровий – функціонування в структурі органів досудового розслідування криміналістичних ІТ-лабораторій, міждисциплінарною компетентністю суб'єктів кримінального провадження, їх профільною спеціалізацією та системним підвищенням кваліфікації; 3) нормативний – використанням єдиних стандартів роботи з доказами досліджуваної категорії, забезпечення їх надійного зберігання та контролю доступу;

– обґрунтування підстав та алгоритмів залучення під час кримінального провадження спеціаліста в сфері цифрової криміналістики в ролі Digital Evidence

First Responder з метою ідентифікації, збирання, здобуття, збереження відповідно до ДСТУ ISO/IEC 27037:2017 із процесуальною цифрових слідів без проведення експертного дослідження. Водночас процесуальну роль експерта пропонується зосереджувати на комплексних дослідженнях, що оптимізує навантаження експертних установ і скоротить строки проведення експертних досліджень;

– підходи до впровадження зарубіжного досвіду роботи з доказами електронної форми, результатами аналізу якого встановлено такі загальні тенденції: інституціоналізація правового режиму доказів електронної форми у межах кримінального процесуального законодавства; утвердження технологічно нейтрального підходу до їх оцінки та допустимості (відсутність вимог визначених технічних засобів чи форматів); посилення вимог до автентичності, цілісності й простежуваності; запровадження спеціальних процесуальних механізмів для їх збирання, збереження та перевірки; уніфікація національних підходів із міжнародними стандартами. У зв'язку з цим у сфері міжнародного обміну доказами електронної форми пропонується: 1) створення комплексної та надійної системи їх захисту; 2) зокрема, розроблення й уніфікація стандартних протоколів та процедур для гармонізації правових аспектів обміну доказами електронної форми між різними юрисдикціями; впровадження сучасних систем управління доказами, що забезпечують автоматизовану фіксацію, відстеження та аналіз усіх взаємодій з ними;

– пропозиції щодо вдосконалення організаційних засад роботи з доказами електронної форми у кримінальному процесі України, що передбачає, зокрема уніфікацію підходів до підготовки юридичних та правоохоронних кадрів на рівні вищих навчальних закладів юридичного та правоохоронного профілів; створення криміналістичних ІТ-лабораторій у структурі правоохоронних органів; результативне професійне навчання суб'єктів кримінального провадження (підвищення кваліфікації), зокрема запровадження міжвідомчих програм підвищення кваліфікації; посилення взаємодії між суб'єктами кримінального провадження – узгодженість у процесуальних діях, обмін знаннями та ресурсами, залучення спеціалістів і створення сталих каналів комунікації між слідчими,

прокурорами, спеціалістами, експертами та судом, модернізацію процедури здійснення тимчасового доступу до речей і документів;

– підходи до вдосконалення технічних аспектів роботи з доказами електронної форми у кримінальному процесі України, що передбачає створення комплексної системи забезпечення цілісності, конфіденційності та збережуваності доказів електронної форми: запровадження гешування як механізму підтвердження цілісності доказів електронної форми; врегулювання практики використання електронних процесуальних документів; впровадження практики резервного копіювання доказів досліджуваної категорії, використання надійних електронних носіїв інформації під час фіксації, здатних забезпечити довготривале зберігання даних; криптографічне шифрування цифрових даних, що є доказами; створення відомчих віртуальних сховищ (цифрових архівів) для зберігання резервних копій доказів електронної форми.

Практичне значення одержаних результатів. Обґрунтовані в дисертації положення впроваджені й можуть бути використані у:

науково-дослідній роботі – для подальших наукових досліджень проблем доказів електронної форми у кримінальному процесі України (акти Національної академії внутрішніх справ від 10.07.2025, Київського столичного університету імені Бориса Грінченка від 16.10.2025, ПВНЗ «Європейський Університет» від 20.10.2025);

законотворчій діяльності – шляхом внесення проєктів змін та доповнень до Кримінального процесуального кодексу України та інших законодавчих актів на основі розроблених автором законопроєктів (лист Комітету Верховної Ради України з питань правоохоронної діяльності від 13.11.2025);

діяльності органів кримінальної юстиції – для розроблення та удосконалення відомчих (міжвідомчих) нормативно-правових актів, підготовки методичних рекомендацій з питань доказів електронної форми у кримінальному процесі (акт Департаменту кіберполіції Національної поліції України від 13.11.2025, лист Офісу Генерального прокурора від 21.11.2025);

освітньому процесі – для підготовки наукових, навчальних та науково-практичних тестових завдань і дидактичних матеріалів з курсів кримінального процесуального права та в системі підвищення кваліфікації прокурорів (акти Тренінгового центру прокурорів України від 01.10.2025, Національної академії внутрішніх справ від 10.07.2025, Київського столичного університету імені Бориса Грінченка від 16.10.2025, ПВНЗ «Європейський Університет» від 20.10.2025, листи проєкту «HELP (Human Rights Education for Legal Professionals) for Ukraine including during wartime» Ради Європи від 16.10.2024), проєкту «CyberUA: Strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine» Ради Європи від 30.10.2025.

Особистий внесок здобувача. Дисертація виконана автором самостійно. Усі сформульовані положення та висновки є результатом особистих досліджень автора. Власні теоретичні розробки здобувача після захисту кандидатської дисертації (2018 р.) та в опублікованих у співавторстві основних наукових працях становлять понад 85 %. Наукові доробки співавторів за темою дисертації не використовувались.

Апробація результатів дисертації. Основні положення та висновки дослідження оприлюднені автором у виступах на всеукраїнських і міжнародних науково-практичних конференціях, круглих столах, зокрема: «Актуальні питання судової експертології, криміналістики та кримінального процесу» (м. Київ, 5 листопада 2019 р.); «Інноваційні рішення в сучасній науці, освіті та практиці» (м. Київ, 17-18 листопада 2020 р.); «Кримінальна юстиція в Україні: реалії та перспективи» (м. Львів, 11 червня 2021 р.); «Сучасні виклики та актуальні проблеми судової реформи в Україні» (м. Чернівці, 29 жовтня 2021 р.); «Наукові читання пам'яті Ганса Гросса» (м. Чернівці, 9 грудня 2021 р.); «Сучасні виклики та актуальні проблеми судової реформи в Україні» (м. Чернівці, 21 жовтня 2022 р.); «III Наукові читання пам'яті Ганса Гросса» (м. Чернівці, 8 грудня 2023 р.); «Сучасні виклики та актуальні проблеми судової реформи в Україні» (м. Чернівці, 27 жовтня 2023 р.); «Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини» (м. Київ, 7 грудня 2023 р.);

«Сучасні виклики та актуальні проблеми судової реформи в Україні» (м. Чернівці, 31 жовтня 2024 р.); «Права людини в умовах воєнного стану в Україні: до тижня права і Загальної декларації прав людини» (м. Київ, 10 грудня 2024 р.); «Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій» (м. Чернівці, 20 грудня 2024 р.); «Актуальні проблеми національного законодавства» (м. Кропивницький, 17 квітня 2025 р.); «Пріоритетні шляхи розвитку науки і освіти» (м. Львів, 9–10 травня 2025 р.); «Актуальні питання реформування правової системи» (м. Луцьк, 13–15 червня 2025 р.).

Публікації. Основні положення дисертації опубліковано в 44 наукових працях, серед яких монографія, 19 статей – у виданнях включених МОН України до переліку наукових фахових з юридичних наук, 3 статті – у періодичних виданнях іноземних країн, 3 статті – у виданнях, що індексуються у наукометричних базах даних Scopus і Web of Science, 15 у збірниках тез доповідей, оприлюднених на науково-практичних конференціях та круглих столах.

Структура та обсяг дисертації. Робота складається з анотації, переліку умовних позначень, вступу, п'яти розділів, що містять 20 підрозділів, висновків, списку використаних джерел (540 найменувань на 67 сторінках) та 25 додатків на 117 сторінках. Повний обсяг дисертації становить 617 сторінок, з них основний текст дисертації – 407 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ДОКАЗІВ ЕЛЕКТРОННОЇ ФОРМИ У КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ

1.1. Вітчизняні доктринальні підходи до розуміння доказів та їх властивостей у кримінальному процесі України

Категорія доказів є фундаментальною для теорії кримінального процесу, оскільки саме через неї забезпечується пізнання обставин кримінального правопорушення, обґрунтування процесуальних рішень і реалізація засад кримінального провадження. Вітчизняна кримінальна процесуальна доктрина виробила значний масив наукових підходів до розуміння доказів, їх властивостей та класифікації, які формувалися в умовах різних історичних, методологічних і ціннісних орієнтирів. Системне осмислення цих підходів є необхідною передумовою побудови цілісної теорії доказів, здатної адекватно реагувати на сучасні трансформації кримінального судочинства, зокрема пов'язані з цифровізацією доказової діяльності, та забезпечити внутрішню концептуальну узгодженість подальшого наукового дослідження.

Сучасні доктринальні уявлення про докази в кримінальному процесі України не виникли одномоментно, а є результатом тривалої та багатоступеневої еволюції наукової думки, у межах якої змінювалися підходи до визначення природи доказів, їх ролі в механізмі доказування та критеріїв їх процесуальної значущості. Історико-доктринальний розвиток цієї категорії характеризується послідовною зміною теоретичних моделей. Їх аналіз дозволяє не лише реконструювати логіку становлення наукових концепцій доказів у вітчизняній кримінальній процесуальній науці, а й створює методологічне підґрунтя для їх критичного осмислення, узагальнення та подальшого використання у формуванні сучасного багатовимірного розуміння доказів.

Початковий етап формування наукових уявлень про докази охоплює дореволюційний період, у межах якого докази розглядалися переважно крізь призму судового пізнання та логіки доведення, без чіткого розмежування між фактичними

даними, засобами їх отримання та процесуальною формою закріплення. Для цього періоду характерним було сприйняття доказів як відомостей про факти, що мають значення для вирішення справи, при домінуванні ідей формальної оцінки доказів та обмеженого розуміння ролі суб'єкта доказування. Водночас саме на цьому етапі було закладено підґрунтя для подальшого наукового осмислення доказів як центральної категорії кримінального процесуального права. Варто вказати на праці дореволюційних процесуалістів, на які посилається сучасна доктрина [202, с. 64]: І. Є. Андрієвського, І. Бентама, В. А. Баніна, Я. І. Баршева, С. І. Вікторського, Л. Є. Владімірова, М. В. Духовського, О. А. Квачевського, В. К. Случевського, В. Д. Спасовича, Д. Г. Тальберга, І. Я. Фойницького та ін.

Наступний, радянський етап розвитку кримінальної процесуальної науки, став визначальним для формування класичної теорії доказів, яка справила тривалий вплив на вітчизняну доктрину. У цей період утверджується інформаційно-гносеологічний підхід, відповідно до якого докази визначалися як фактичні дані, що відображають об'єктивну дійсність і встановлюються у передбаченому законом порядку (узагальнюючи положення радянської теорії доказів, викладені у працях М. С. Строговича, С. О. Голунського, В. Я. Дорохова, А. Р. Белкіна та ін.). Саме в межах радянської доктрини було системно розроблено вчення про предмет доказування, процес доказування, а також сформульовано базові уявлення про властивості доказів, насамперед їх належність, допустимість і достовірність. Водночас для цього етапу характерною була надмірна орієнтація на ідею об'єктивної істини та зведення ролі процесуальної форми до інструментального засобу фіксації фактичних даних, що зумовлювало певну методологічну одновимірність підходів до доказів.

Період становлення незалежної України та прийняття нового кримінального процесуального законодавства зумовив перегляд традиційних доктринальних конструкцій і започаткував сучасний етап розвитку теорії доказів. Українська доктрина кримінального процесуального доказування формувалася на засадах класичних теоретичних уявлень, у межах яких доказування осмислювалося як самостійний різновид процесуальної діяльності, спрямованої на збирання, перевірку та оцінку доказів у суворій відповідності до вимог закону. У наукових працях

В. П. Гмирка доказування розкривається як діяльнісна модель, що інтегрує пізнавальний і нормативний компоненти та потребує урахування логіки, структури і функціонального призначення доказової діяльності [52]. Вагомий внесок у розвиток загальнотеоретичних засад доказування зроблено й у працях В. М. Тертишника, який розглядає доказування як комплексну правову категорію, що поєднує пізнання, оцінювання та процесуальні гарантії [268]. У межах класичної процесуальної теорії О. В. Капліна [130], Є. Г. Коваленко [138] та С. М. Стахівський [254] зосереджували увагу на системі доказів, їх процесуальних джерелах і властивостях, а також на внутрішньому переконанні суду як визначальному чиннику оцінки доказового матеріалу. Доктринальні основи доказів у кримінальному процесі України системно розвинули: В. В. Вапнярчук [26; 27], О. В. Капліна [131], С. О. Ковальчук [139], М. А. Погорецький [192; 193; 194; 195; 196; 197; 198; 199; 200; 201; 202; 203; 204; 205; 206; 207; 208; 209; 210; 211; 212; 213], О. С. Старенький [253; 202; 49], Д. Б. Сергєєва [245; 246; 247], та інші вчені. Також варто відзначити творчий спадок О. Г. Шилю [237].

Подальша еволюція доктрини пов'язана з переорієнтацією на проблеми допустимості, належності та оцінки доказів у контексті прийняття чинного Кримінального процесуального кодексу України (далі – КПК України). У цьому аспекті істотне значення мають дослідження Д. Б. Сергєєвої, в яких допустимість обґрунтовується як самостійна властивість доказу та розкривається її співвідношення з належністю та достовірністю [245; 246; 247]. М. Є. Шумило аргументував необхідність чіткого доктринального розмежування доказів і процесуальних рішень, що має принципове значення для правильної оцінки допустимості доказового матеріалу [294]. Праці О. С. Старенького зосереджені на процесуальних гарантіях сторони захисту у збиранні та використанні доказів, що посилює змагальний вимір доказування [253]. Водночас В. В. Вапнярчук [26; 27] і Г. Р. Крет [151] розвинули концепцію стандартів доказування, наголошуючи на їх узгодженні з принципами справедливого судового розгляду. Окремий напрям сучасних досліджень пов'язаний з аналізом логіки формування доказової бази та методології доказування, у межах якого доказ розглядається як елемент цілісної

системи аргументації у кримінальному провадженні, здійснений у працях О. І. Гвоздіка та О. С. Старенького [49]. М. А. Погорецьким сформовано цілісний авторський доктринальний підхід до кримінального процесуального доказування, у межах якого обґрунтовано функціональний зв'язок оперативно-розшукової діяльності, негласних заходів і процесуальної форми кримінального провадження як передумови легалізації результатів аналітичної та доказової діяльності [201; 202; 207; 208; 209].

Загалом аналіз наукових джерел свідчить про послідовну трансформацію української доктрини доказування від класичних процесуально-формальних моделей до конституційно орієнтованої концепції, у межах якої доказове право розглядається як інструмент забезпечення та захисту прав людини.

Історико-доктринальний аналіз засвідчує, що категорія доказів у вітчизняній кримінальній процесуальній науці зазнала суттєвої еволюції — від спрощеного уявлення про докази як відомості про факти до сучасного комплексного розуміння доказів як результату нормативно врегульованої пізнавальної діяльності, обмеженої вимогами процесуальної форми та орієнтованої на забезпечення прав і свобод людини. Усвідомлення цієї еволюції є необхідною методологічною передумовою для подальшого аналізу наукових моделей доказів і формування цілісної концепції доказів електронної форми у кримінальному процесі України.

Еволюція вітчизняної теорії доказів у кримінальному процесі України зумовила формування низки наукових моделей розуміння доказів, кожна з яких відображає окремий аспект цієї складної правової категорії. Зазначені моделі різняться за вихідними методологічними передумовами, предметними акцентами та межами пояснювального потенціалу, що об'єктивно потребує їх системного аналізу, критичного співвіднесення та подальшого доктринального узагальнення.

У межах інформаційної моделі (одним із провідних розробників вважається В. Я. Дорохов) доказ у кримінальному процесі осмислюється передусім через його інформаційний зміст — фактичні дані (відомості) про обставини кримінального правопорушення, які мають значення для встановлення предмета доказування. Теоретичним підґрунтям цієї моделі є гносеологічний підхід до кримінального

процесу, відповідно до якого доказування розглядається як пізнавальна діяльність, спрямована на відтворення фактичної картини події. Процесуальна форма в межах цієї моделі виконує похідну функцію та розглядається переважно як засіб (умова) введення та перевірки фактичних даних у процедурі доказування. Предметні акценти інформаційної моделі зосереджуються на інформаційній природі доказу, відмежуванні його змісту від джерела та пізнавальній функції доказування. Водночас внутрішнім обмеженням інформаційної моделі є тенденція до редукції доказу виключно до його змістовної складової, що ускладнює врахування процесуальних гарантій допустимості, стандартів доказування та прав людини як системоутворювальних елементів доказової діяльності.

Процесуальна (формально-процесуальна) модель, виходить із протилежної методологічної установки, відповідно до якої доказом може бути визнано лише ті відомості, що набули доказового статусу внаслідок дотримання встановленої кримінальним процесуальним законом процедури (відповідні положення відображені в роботах таких науковців як М. Є. Шумило, В. М. Тertiшник, Д. Б. Сергеева та інші). Процесуальна форма в цій моделі не є похідною від змісту доказової інформації, а виступає визначальним чинником її юридичної легітимації. У центрі уваги перебувають допустимість як ключова властивість доказів, процесуальні джерела доказів і судовий контроль за дотриманням процедури їх отримання. Водночас ризиком формально-процесуальної моделі є гіперформалізація доказування, за якої змістова достовірність і переконливість доказів можуть поступатися формальній відповідності встановленій процедурі.

У межах матеріальної моделі (або ж матеріально-правової) докази розглядаються через їх функціональний зв'язок із предметом доказування, який визначається у тісному зв'язку з кримінально-правовою характеристикою події та обставинами, що підлягають доказуванню. В цій парадигмі доказування (підхід характерний для таких авторів як П. С. Елькінд, М. С. Строгович) підпорядковується завданням встановлення юридично значущих матеріальних обставин та забезпечення належної кримінально-правової кваліфікації. Основними предметними акцентами є релевантність доказів до елементів складу кримінального

правопорушення та їх спрямованість на підтвердження чи спростування матеріально-правових фактів. Водночас внутрішнім обмеженням матеріально-правової моделі є ризик матеріально-правової редукції, коли автономія процесуальної форми та гарантій доказування нівелюється на користь кінцевого результату кримінально-правової оцінки.

Аксіологічна модель виходить із того, що доказування є не лише пізнавальною, а й ціннісно зумовленою діяльністю, спрямованою на досягнення справедливого результату в межах установлених процесуальних стандартів. У центрі цієї моделі (використовують Ю. К. Орлов та частково М. М. Михеєнко) перебувають баланс між істиною і справедливістю, а також обґрунтованість і переконливість судових рішень як прояв легітимності правосуддя. Разом із тим аксіологічна модель потребує чіткої процесуальної конкретизації, оскільки без належної нормативної операціоналізації існує ризик її декларативності.

Особливе місце в сучасній доктрині посідають конституційно орієнтовані підходи, у межах яких доказування розглядається крізь призму примату прав і свобод людини (обґрунтовує О. С. Старенький, підтримують М. А. Погорецький та В. М. Тертишник). Вихідною теоретичною передумовою цих підходів є визнання прав людини системоутворювальним чинником доказової діяльності, що визначає межі допустимого державного втручання. Предметні акценти зосереджуються на допустимості доказів як похідній від дотримання прав людини, судовому контролю та стандартах справедливого судового розгляду, вироблених у практиці Європейського суду з прав людини, які впливають на оцінку допустимості та процесуальних наслідків порушень прав людини.

В. В. Вапнярчук (2018) вважає, що найбільш продуктивною й такою, що повною мірою розкриває сутнісну правову природу поняття «докази» є модель (трактування), яка відображає такі основні сторони: інформаційну (відомості), матеріальну (процесуальні джерела), логічну (факт, пізнаний з допомогою відомостей, що містяться в певному джерелі, відрізок об'єктивної дійсності) та процесуальну (процедурну) (визначений законом порядок отримання відомостей про факти й порядок їх закріплення у процесуальних джерелах). На думку

В. В. Вапнярчука, для такої моделі найбільше підходить назва «комплексно-системна» [26, с. 256-257]. Вказана ідея, на нашу думку, вбачається вдалою.

М. А. Погорецький обґрунтовує інтегративний (комплексний) підхід до розуміння доказу, відповідно до якого доказ у кримінальному процесі є єдністю фактичних даних, їх джерел та процесуальної форми, що набувають доказового значення внаслідок реалізації уповноваженими суб'єктами кримінального провадження передбачених законом процесуальних повноважень [196, с. 33-43]. Інтегративний підхід, запропонований М. А. Погорецьким, має принципове значення для подальшого дослідження доказів електронної форми, оскільки дозволяє розглядати цифрові відомості не як самостійний різновид доказів, а як інформаційний компонент, що набуває доказового значення лише за умови належного процесуального оформлення, закріплення у визначених законом джерелах і перевірки в установленій кримінальним процесуальним законом процедурі.

У критичному вимірі наведені наукові моделі доцільно розглядати не як взаємовиключні, а як такі, що висвітлюють різні сторони складної та багатовимірної категорії доказів. Інформаційна модель розкриває пізнавальну природу доказування; формально-процесуальна – його юридичну легітимність; матеріально-правова – функціональну спрямованість на предмет доказування; аксіологічна – ціннісну вмотивованість і мету; конституційно орієнтована – межі допустимого державного втручання та гарантії справедливості. Водночас абсолютизація будь-якої з цих моделей неминує породжує редукціонізм (інформаційний, формалістичний, матеріально-правовий або ціннісний), який у сучасних умовах має бути подоланий. У подальшому дослідженні докази електронної форми розглядатимуться саме крізь інтегративну призму зазначених моделей: інформаційна складова пояснює природу цифрових відомостей, формально-процесуальна та конституційно орієнтована – критерії їх допустимості та гарантії прав людини, а матеріально-правова й аксіологічна – релевантність їх використання. Такий підхід дозволяє уникнути як технократичної редукції доказу до цифрового об'єкта, так і абстрактного правового

формалізму без процедурної верифікації цілісності, автентичності та ланцюга збереження доказів.

Узагальнення доктринальної еволюції дозволяє дійти висновку, що категорія доказів у вітчизняній кримінальній процесуальній науці не є одновимірною. Її сучасне розуміння є результатом тривалого розвитку наукової думки, у межах якого доказ осмислюється як багатовимірна категорія, що поєднує інформаційний зміст, процесуальну форму, матеріально-правову релевантність, аксіологічні орієнтири та конституційно-правові гарантії. Саме таке інтегративне бачення створює належне методологічне підґрунтя для подальшого дослідження доказів електронної форми у кримінальному процесі України.

Окреслення історико-доктринальних етапів розвитку уявлень про докази та виділення базових методологічних моделей їх розуміння створюють необхідну рамку для подальшого, більш предметного аналізу сучасних наукових позицій.

В. В. Вапнярчук (2018) аналізує періодизацію Р. В. Костенка, який запропонував еволюцію поглядів з питання про поняття доказів умовно поділяти на три періоди розвитку: перший – це погляди дореволюційних юристів (до 1917 р.); другий – радянський період (1917– 1991 рр.); третій – сучасні погляди науковців (з 1991 р. до сьогодні). Водночас, вченим підкреслено сумнівність цієї періодизації. Як більш вдала альтернатива В. В. Вапнярчуком (2018) представлена концепція Ю. К. Орлова щодо моделей поняття «докази». Узагальнивши позиції різних учених останній виокремив п'ять основних трактувань, серед яких: 1) донаукове; 2) логічне; 3) «двоїсте»; 4) інформаційне; 5) змішане (синтезоване) [26, с. 253].

На думку В. В. Вапнярчука (2018) наведена концепція загалом заслуговує на підтримку, однак потребує окремих уточнень і доповнень. Її зміст доцільно подати у стислому вигляді з урахуванням доктринальних зауважень. Донаукове трактування доказів характерне для початкового етапу розвитку теорії доказів, коли наукове поняття ще не було сформоване (до прийняття в 1958 р. Основ кримінального судочинства СРСР і союзних республік). У межах цієї моделі докази сприймалися на побутовому рівні — як усе, що сприяє встановленню обставин справи. Логічна модель сформувалася після законодавчого закріплення поняття

доказів як фактичних даних у ст. 16 Основ 1958 р. Її прихильники ототожнювали докази виключно з фактами, розуміючи їх як пізнаний відрізок дійсності або достовірне знання, що слугує логічним аргументом у доказуванні. Водночас ця модель зазнала обґрунтованої критики через ігнорування джерел доказів і проблеми їх оцінки. «Двоїсте» трактування виникло як реакція на обмеження логічної моделі й передбачало визнання доказами як самих фактів, так і їх процесуальних джерел (показань, документів, речових доказів тощо). Попри певні переваги, така модель також не забезпечила вичерпного розкриття сутності доказів. Інформаційна модель, розроблена В. Я. Дороховим, розглядала доказ як єдність відомостей про факти та джерел цих відомостей. Її перевагою стало обґрунтування можливості перевірки, оцінки та встановлення достовірності інформації. Разом із тим модель зосереджувалася переважно на інформаційному аспекті, залишаючи поза увагою логічну складову доказування. Змішана (синтезована) модель поєднала факти, відомості про них і джерела таких відомостей, охоплюючи як інформаційну, так і логічну сторони доказування. Водночас, як зауважував Ю. К. Орлов, використання єдиного терміна «докази» для різних ґносеологічних категорій створює ризик термінологічної нечіткості. Окремої уваги заслуговує системна модель, запропонована В. С. Балакшиним, яка розглядає докази як систему взаємопов'язаних елементів: фактичних даних, їх джерел і процедур збирання, закріплення та перевірки. Її позитивом є врахування процесуальної природи доказування, тоді як недоліком – відсутність чіткого відображення логічної складової, що загалом зближує її з інформаційною моделлю [26, с. 253-256].

В. П. Гмирко (2014) запропонував характеризувати доказ як результат мислєдіяльностних операцій людини, що складається з пізнавального, інформаційного і нормативного сегментів» [53, с. 34].

Ми поділяємо думку А. М. Погорецького, О. С. Старенького, які визнають існування теорії кримінального процесуального доказування як самостійної теорії кримінального процесу, а теорію доказів її складовою [203; 204, с. 309].

М. Є. Шумило (2018) пропонує розглядати доказ, як юридичну конструкцію, яка включає такі структуровані сегменти: 1. Нормативно-процедурний. Цей елемент

конструкції процесуального доказу встановлює вимоги до нормативної процедури отримання доказів, а також стандартів щодо засобів і порядку їхнього допуску до процесу доказування. Так, в ч. 1 ст. 84 КПК України вказується, що: 1) докази – це фактичні дані; 2) їх отримання має відбуватися у передбаченому Кодексом порядку; 3) фактичні дані повинні мати юридично-пізнавальне значення для кримінального провадження. Крім цього, в КПК України сформульовано вимоги щодо належності (ст. 85), допустимості (ст. 86) і недопустимості доказів (ст.ст. 87, 88); 2. Знаннєвий. У структурі діяльності по формуванню доказів запроваджено процесуальні механізми забезпечення сторін і суду певними відомостями, на підставі яких можуть бути встановлені доказові факти. Носієм таких даних завжди є конкретна особа, яка їх осмислює і перетворює у знання. Це свідчить про те, що формування доказу є осмисленим конструюванням моделі реальності з використанням когнітивних структур (схем, стереотипів, світогляду) в сприйнятті й переосмисленні відомостей. Зусилля суб'єкта пізнання концентруються на отриманні структурованого знання у формі знаннєвих одиниць—фактів. Тому являються хибними ствердження про те, що доказами є інформація (фактичні дані). Вона не має смислу і не пов'язана з конкретною особою та передається від одного технічного пристрою до іншого; 3. Судово-інтерпретаційний. КПК України передбачив двохступеневу процедуру формування доказів на досудову і судову. Згідно ч. 1 ст. 84 КПК України фактичні дані можуть визнаватися доказами слідчим і прокурором у стадії досудового розслідування. Водночас на рівні засади кримінального процесу у ч. 2 ст. 23 КПК України вказується, що «не можуть бути визнані доказами відомості, що містяться в показаннях, речах і документах, які не були предметом безпосереднього дослідження суду». Докази, сформовані слідчим і прокурором, представниками обвинувальної влади, не придатні для вирішення питання винуватості особи у вчиненні злочину. Тому вони потребують дослідження в умовах судового розгляду за участі сторін і суду. Змагальна процедура покликана відкорегувати представлені сторонами докази, очистити від суб'єктивно-хибних нашарувань і визначити їх реальну доказову силу; 4. Фактовстановлюючий. За результатами різностороннього судового обговорення (інтерпретації) судом визнається судовий доказ як колективне

юридично значиме знання (факт), придатне з позицій справедливості, совісті, достовірності, належності та допустимості підтверджувати чи спростовувати обставини, що підлягають доказуванню [295, с. 65-66].

В. В. Вапнярчук (2018) висловлює позицію, що фактичні дані можуть набувати статусу доказу для конкретного суб'єкта (сторони обвинувачення або сторони захисту) відразу — за умови їх збирання у порядку, визначеному КПК України, та за наявності інших властивостей доказів і дотримання критеріїв допустимості. Однак для інших суб'єктів і для кримінального провадження загалом такі дані набувають статусу доказів лише після їх одержання у передбаченому законом порядку суб'єктами, прямо зазначеними в ч. 1 ст. 84 КПК України (слідчим, прокурором, слідчим суддею або судом), які здійснюють кримінальне провадження [26, с. 257].

Конструкцію такої моделі можемо знайти й у визначенні поняття доказів у ст. 84 чинного КПК України. Під фактичними даними В. В. Вапнярчук (2018) пропонує розуміти відомості про факти (інформаційна сторона); у фразі «отримані у передбаченому цим Кодексом порядку» йдеться про процесуальну сторону доказування; словосполучення «встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження» свідчить про логічну сторону сутності поняття доказів; перелік же можливих процесуальних джерел доказів (ч. 2 ст. 84 КПК України) підкреслює його матеріальну сторону [26, с. 257].

На нашу думку доцільно підтримати позицію А. М. Погорецького як найбільш релевантну в контексті подальшого дисертаційного дослідження. А. М. Погорецький (2011) вказує, що досліджуючи докази та доказування, одні правознавці (В. Я. Дорохов, Ф. Н. Фаткуллін, В. І. Зажицький, Н. В. Сібілєва, Е. А. Доля) вважають, що це категорії, властиві лише стадіям досудового розслідування та судовим стадіям, на думку інших (Л. М. Карнеєв, Н. П. Кузнецов, С. М. Стахівський), доказування відбувається й на стадії порушення провадження у кримінальній справі, а тому доказами оперують і на цій стадії кримінального процесу. Така розбіжність думок у принципових питаннях доказового права призводить до неоднозначності закріплення окремих його категорій у законодавстві, до неоднакового їх розуміння правозастосовниками і як наслідок — до неефективності кримінальної юстиції та до

судово-слідчих помилок, що нерідко грубо порушують права людини у кримінальному судочинстві [196, с. 2], з чим варто погодитись.

Проведений А. М. Погорецьким (2011) системно-логічний аналіз різноманітних точок зору численних науковців на поняття доказу в кримінальному процесі дає підстави для висновку, з яким автор погоджується, що найбільш обґрунтованою та такою, що відповідає його ґносеологічній та правовій природі, є концепція судового доказу як єдності фактичних даних та їх процесуальних джерел. Вчений вказує, що для всебічного дослідження доказу у кримінальному процесі як єдності фактичних даних та їх процесуальних джерел, як окремий елемент цієї єдності слід виділяти також і його процесуальну форму. У цьому є сенс, оскільки, навіть тоді, коли є, наприклад, сукупність фактичних даних, що вказують на наявність або відсутність суспільно небезпечного діяння, та їх процесуальних джерел, такі фактичні дані можуть бути не визнані доказами, якщо грубо порушена процесуальна форма їх отримання чи джерело фактичних даних не відповідає вимогам, які ставляться до джерел доказів. Процесуальна форма доказування в широкому розумінні визначається як система встановлених законом правил, відповідно до яких здійснюється доказування на всіх стадіях кримінального процесу. Вона охоплює: принципи кримінального судочинства тією мірою, в якій вони відбиті в доказовому праві й діяльності по доказуванню; поняття й інститути доказового права, побудовані відповідно до цих принципів (предмет доказування, поняття доказу, засоби доказування); особливості інститутів доказового права на окремих стадіях процесу й у деяких категоріях кримінальних справ; коло органів і осіб, що беруть участь у доказуванні, їхні права й обов'язки. У вузькому розумінні процесуальна форма конкретного доказу у кримінальному процесі — це встановлений порядок його отримання й закріплення у відповідному процесуальному документі, що забезпечує можливість перевірки процесу його отримання й робить його таким, що є належним і допустимим. Процесуальна форма кожного доказу має своє відображення у відповідному процесуальному документі [196, с. 31-32].

Три елемента: фактичні дані, їх джерела та процесуальна форма, маючи взаємовпливовий та взаємозалежний зв'язок, у своїй єдності становлять поняття як процесуального доказу загалом, так і доказу у кримінальній справі зокрема. Відсутність будь-якого із зазначених елементів, наприклад, грубе порушення процесуальної форми отримання відповідного доказу чи відсутність фактичних даних, які можуть бути визнані доказами, або їх джерела, робить доказ таким, що втрачає свою сутність. Водночас надання фактичним даним статусу доказу можливе лише в результаті пізнавально-процесуальної діяльності уповноважених суб'єктів кримінального провадження, які здійснюють їх збирання, перевірку, оцінку та процесуальне закріплення у межах наданих законом повноважень. Саме через діяльність такого суб'єкта забезпечується реальна єдність фактичних даних, їх джерел і процесуальної форми та набуття ними юридичного значення доказу у конкретному кримінальному провадженні [196, с. 33-43]. Наведена позиція видається обґрунтованою.

Докази і доказова інформація є самостійними поняттями, які мають єдину гносеологічну природу, проте різний правовий статус. Доказова інформація — це та інформація (фактичні дані), яка, хоча й отримана з відповідних джерел, проте ще не набула статусу доказів у кримінальному процесі. Доказова інформація має велике значення для кримінального процесу, оскільки вона за певних умов може бути використана як для отримання певних доказів, так і для прийняття окремих процесуальних рішень у кримінальному процесі. А. М. Погорецьким (2011) вказує, що з цього питання цілком переконливим є висновок І. М. Лузгіна, що субстанцію судового доказу справді утворює інформація. Однак для визначення поняття доказу в кримінальному процесі поняття сигналу інформації не може бути використане, бо воно характеризує спосіб передачі інформації, її переміщення в часі й просторі, але не розкриває правової природи судового доказу. Як слушно зазначав М. М. Михеєнко, використання окремих положень теорії інформації для розкриття сутності кримінально-процесуального доказу може бути плідним лише тоді, коли при цьому не забувається юридична природа зазначених доказів [196, с. 37].

Поділяючи вказану позицію варто вказати на її істотний вплив на подальше дослідження та пропозиції, що висловлюються в роботі.

Нормативне закріплення співвідношення доказів і джерел доказів у чинному Кримінальному процесуальному кодексі України здійснене насамперед у ст. 84 КПК України, яка містить легальне визначення доказів та одночасно фіксує вичерпний перелік їх процесуальних джерел. Законодавець виходить із конструкції, відповідно до якої доказами у кримінальному провадженні є фактичні дані, отримані у передбаченому Кодексом порядку, а встановлення цих фактичних даних здійснюється через конкретні процесуальні джерела. До таких джерел закон прямо відносить показання, речові докази, документи та висновки експертів. Отже, нормативна модель доказу в чинному КПК України ґрунтується на чіткому розмежуванні між фактичними даними як змістовною стороною доказу та процесуальними джерелами як формою їх існування і закріплення в кримінальному процесі.

Доктринальна інтерпретація цього співвідношення в сучасній українській науці кримінального процесу є неоднорідною, однак домінуючою залишається концепція, запропонована А. М. Погорельським, відповідно до якої доказ у кримінальному провадженні розглядається як єдність фактичних даних, їх джерела та процесуальної форми, а набуття доказового значення зумовлюється реалізацією уповноваженими суб'єктами кримінального провадження передбачених законом процесуальних повноважень. Саме така інтерпретація дозволяє узгодити нормативний текст ст. 84 КПК України з гносеологічною природою доказування, забезпечивши поєднання інформаційної, логічної та процесуальної складових доказу.

У межах даного дисертаційного дослідження обґрунтовується наукова модель, відповідно до якої кожному з чотирьох процесуальних джерел доказів, закріплених у ст. 84 КПК України, кореспондує самостійний вид доказів, при цьому електронна форма є універсальною характеристикою, притаманною всім цим видам, що детально висвітлюється в наступних підрозділах дисертаційного дослідження.

Такий підхід не заперечує традиційного поділу джерел доказів, а, навпаки, розкриває їх сучасний функціональний потенціал у цифровому середовищі.

Методологічною перевагою запропонованого підходу є його інтегративний характер. Він не спрямований на руйнування усталених у науці кримінального процесу конструкцій доказу та джерел доказів, а передбачає їх концептуальну інтеграцію в існуючі доктринальні моделі. Застосування електронної форми як наскрізної характеристики різних видів доказів дозволяє зберегти нормативну стабільність інституту доказів і водночас адекватно відобразити об'єктивні трансформації способів фіксації, зберігання та передачі фактичних даних у сучасному кримінальному процесі.

Запропонована модель має значний потенціал для подолання доктринальних суперечностей, що традиційно виникають у зв'язку з розмежуванням понять «докази», «доказова інформація» та «джерела доказів». Визнання того, що електронна форма є способом існування фактичних даних у межах уже визначених законом процесуальних джерел доказів, дозволяє уникнути термінологічної плутанини та забезпечити доктринальну послідовність і сталість у тлумаченні інституту доказів. Такий підхід узгоджується як з нормативним текстом КПК України, так і з положеннями сучасної теорії кримінального процесуального доказування.

Водночас, цифрова природа даних має відповідний потенціал (з урахуванням перспектив розвитку інформаційних технологій), водночас, по-перше, не може бути реалізована на сучасному етапі розвитку кримінального процесу України (адже маж бути забезпечено поступовість та сталість, особливо в частині забезпечення підтвердження цілісності та автентичності даних електронної (цифрової) природи), а по-друге – не є предметом цього дисертаційного дослідження.

Відтак, запропоноване авторське позиціонування має визначальне значення для забезпечення цілісності всієї теорії доказів електронної форми, що розробляється в дисертації. Воно створює концептуальне підґрунтя для подальшого аналізу. Завдяки цьому теорія доказів електронної форми постає не як альтернативна або паралельна конструкція, а як внутрішньо узгоджений елемент загальної теорії

кримінального процесуального доказування, що відповідає як вимогам юридичної науки, так і потребам сучасної правозастосовної практики.

Вживання терміна «властивість» можливе лише до тих ознак відомостей про обставини справи, які є невід’ємними від сутності феномена доказу. Прийнятним є використання в цьому разі відомої аксіоми: якщо, за відсутності деяких ознак, існування певного явища можливе без змін, це означає, що ці ознаки не відображають істинної сутності явища. Властивостями доказів у кримінальному процесі є їх належність та допустимість, які характеризують зміст та форму доказів відповідно. Термін «характеристика» уявляється прийнятним для визначення іншої ознаки – достовірності. Достатність виступає властивістю системи доказів, компонентами якої є: логічна послідовність, однозначність висновків, погодженість і несуперечність доказів і встановлених обставин, стійкість знання, повнота встановлених обставин предмета доказування, інваріантність [256, с. 13-14].

Д. Б. Сергєєва (2015) слушно вказує, що не всі отримані докази можуть використовуватися у кримінальному судочинстві, у тому числі й для обґрунтування вироку, а лише ті, що мають такі внутрішні властивості, як належність, допустимість та достовірність. Вищевказані та інші властивості доказів (сила, значимість, достатність тощо), що виокремлюються окремими фахівцями (Ю. К. Орлов), їх зміст та критерії визначення є дискусійними яку теорії доказів, так і в науці кримінального процесу в цілому [245, с. 80].

Варто погодитися з М. М. Стояновим (2010), що структура дослідження доказів, схематично відображена як «належність – допустимість – достовірність – достатність», визначає механізм та послідовність встановлення властивостей доказів. Між належністю доказів та їх достовірністю існує однобічний зв’язок. Тільки належний доказ може бути визнано достовірним. Належність доказу не вирішує заздалегідь питання про його достовірність. Тобто належні відомості можуть бути як достовірними, так і недостовірними. Належність відомостей створює лише потенційну можливість для встановлення їх достовірності. Зв’язок допустимості з належністю не простежується. Правила допустимості доказів покликані гарантувати дотримання прав учасників процесу при збиранні доказової

інформації та забезпечити достовірність одержаних відомостей. Недотримання цих правил тягне за собою виникнення сумнівів різного ступеня істотності в достовірності отриманої інформації. Таким чином, правила допустимості доказів забезпечують їх достовірність. У той самий час висновок про допустимість передуює, але не заміняє висновку про достовірність доказу [256, с. 15].

В. В. Вапнярчуком (2018) як властивості доказів виокремлені й проаналізовані належність, допустимість, достовірність та значущість (сила) (притаманні кожному доказу) та достатність і взаємозв'язок (характерні для сукупності доказів) [26, с. 316-317].

На нашу думку, властивості доказів у кримінальному процесі утворюють не просту сукупність окремих ознак, а внутрішньо впорядковану систему, що має власну логіку, ієрархію та функціональне призначення в механізмі кримінального процесуального доказування. Належність, допустимість, достовірність і достатність не існують ізольовано, а перебувають у відносинах взаємозумовленості, послідовності та функціональної взаємодії, що визначає як порядок їх встановлення, так і межі використання доказів у процесуальній діяльності.

Під належністю доказів слід розуміти можливість використання їх для встановлення у кримінальному провадженні фактичних даних (відомостей про факти), а також обставин, що підлягають доказуванню в силу існуючого між ними кримінального процесуального взаємозв'язку. Головним для визнання належним доказу у кримінальному провадженні має вирішення питання про те, чи належать обставини і факти, для встановлення яких він використовується, до кола тих, котрі мають істотне значення для правильного вирішення кримінального провадження і, тим самим, підлягають доказуванню. Якщо належать, значить відповідають вимозі належності, а якщо не належать, то такій вимозі не відповідають і тому доказуванню не підлягають. При цьому, для визнання доказу у провадженні не має значення, чи входять обставини і фактичні дані, ними встановлені, у коло тих компонентів предмета доказування, що безпосередньо передбачено ст. 91 КПК України, чи сформульовані вони в інших статтях КПК України або відносяться до числа так званих «проміжних» фактичних даних і обставин, на підставі яких можуть бути

встановлені складові предмета доказування, оскільки всі вони в кінцевому підсумку складають предмет доказування [141, с. 12].

Допустимість доказу в кримінальному процесі України є однією з ключових категорій інституту доказування (досліджена в численних дисертаційних дослідженнях [251; 141; 92; 288; 274; 255; 39]) і тісно пов'язана із суворим дотриманням процесуальних приписів на всіх його етапах.

М. А. Погорецький (2007) під допустимістю доказів розуміє таку внутрішню властиву їм якість, внаслідок якої ці докази здатні встановити обставини, що необхідні для повного й правильного вирішення певного кримінального провадження, а вимога належності охоплює не весь доказ у цілому, а лише його змістовну частину – фактичні дані. Вимоги, що ставляться законом до процесу отримання доказів, становить інститут процесуальної допустимості, який полягає в тому, що належні до кримінального провадження фактичні дані повинні бути одержані із встановленого законом джерела, уповноваженим на це суб'єктом кримінального процесу і закріплені у спосіб, вказаний у кримінальному процесуальному законі [206, с. 487-488, 490-491].

Вважаємо, що внутрішня логіка системи властивостей доказів полягає насамперед у їх ієрархічному зв'язку. Належність і допустимість виступають первинними властивостями, без встановлення яких подальша оцінка доказів втрачає сенс. Належність визначає змістовну релевантність відомостей до предмета доказування, окреслюючи межі допустимого доказового матеріалу з погляду його зв'язку з юридично значущими обставинами. Допустимість, своєю чергою, забезпечує формально-процесуальну легітимність доказів, фіксуючи відповідність способів їх одержання, закріплення та використання вимогам кримінального процесуального закону. Лише за наявності цих двох властивостей можливе звернення до питання достовірності доказу як відповідності його змісту об'єктивній дійсності.

Достовірність у цій системі займає особливе місце, оскільки вона є характеристикою окремого доказу, але встановлюється лише в контексті аналізу всієї сукупності доказів. Вона не може бути виведена ані з належності, ані з

допустимості автоматично, хоча останні створюють необхідні умови для її перевірки. Саме тому висновок про достовірність є результатом складної інтелектуально-оціночної діяльності суб'єктів доказування, що спирається на принципи всебічності, повноти та об'єктивності дослідження обставин кримінального провадження.

Достатність доказів являє собою їх системну процесуальну властивість, у зв'язку з чим її встановленню передуює оцінка доказів із точки зору індивідуальних процесуальних властивостей, якими виступають: 1) належність доказів, яка являє собою їх процесуальну властивість, що відображає наявність зв'язку між їх змістом та обставинами, що підлягають доказуванню; 2) допустимість доказів, яка становить їх процесуальну властивість, що вказує на отримання доказів із дотриманням встановлених КПК України вимог стосовно належного джерела, належного суб'єкта і порядку одержання; 3) достовірність доказів, яка являє собою їх процесуальну властивість, що відображає відповідність змісту доказів об'єктивній дійсності та їх придатність для використання для встановлення обставин, які мають значення для кримінального провадження та підлягають доказуванню [89, с. 178-179].

Достовірність – це відповідність доказу об'єктивній дійсності, його безсумнівність, обумовлені проведенням кримінально-процесуальним дослідженням. Висновок про достовірність окремого доказу можна зробити лише після дослідження всіх зібраних у справі доказів у їх системі. У той самий час достовірність є характеристикою окремо взятого доказу, а не їх сукупності. Перетворення імовірності на достовірність супроводжує процес доказування у справі. Сумніви в процесі побудови слідчих версій, збирання доказів виправдані з позиції всебічного, повного та об'єктивного встановлення обставин справи. Але використовуватися для прийняття процесуальних рішень повинні лише докази, достовірність яких після їх дослідження не викликає в суб'єктів доказування будь-яких сумнівів. У той самий час, внаслідок закріплення та дії принципу презумпції невинності, суб'єкти доказування, що представляють сторону захисту, мають право використовувати в кримінальному процесі дані, у достовірності яких вони не

переконані. Суб'єкти доказування, які ведуть або ініціюють кримінальний процес, такого права не мають [256, с. 14].

Достатність, на відміну від інших властивостей, має виразно системний характер і стосується не окремого доказу, а всієї доказової сукупності. Вона відображає досягнення такого рівня узгодженості, повноти та переконливості доказів, який дозволяє зробити однозначні висновки щодо обставин, що підлягають доказуванню, і прийняти законне та обґрунтоване процесуальне рішення. У цьому сенсі достатність інтегрує результати встановлення належності, допустимості та достовірності, виконуючи завершальну функцію в структурі доказування.

Функціональне призначення системи властивостей доказів проявляється в тому, що кожна з них виконує самостійну, але взаємопов'язану роль у механізмі кримінального процесуального доказування. Належність орієнтує доказову діяльність на предмет доказування та запобігає залученню до процесу відомостей, що не мають юридичного значення. Допустимість забезпечує дотримання процесуальних гарантій, захист прав і свобод учасників кримінального провадження та легітимність втручання держави у сферу приватних інтересів. Достовірність слугує критерієм пізнавальної надійності доказів і передумовою формування внутрішнього переконання суду. Достатність, у свою чергу, забезпечує перехід від оцінки окремих доказів до прийняття підсумкового рішення, поєднуючи пізнавальний і нормативний виміри кримінального процесу.

Системне розуміння властивостей доказів має принципове значення для зв'язку загальної теорії доказів із дослідженням їх окремих видів. Саме універсальність властивостей належності, допустимості, достовірності та достатності дозволяє застосовувати єдині теоретичні критерії до різних доказових форм, незалежно від їх джерела, способу фіксації чи матеріального носія. Водночас особливості окремих видів доказів зумовлюють специфіку реалізації цих властивостей, що потребує доктринального уточнення без руйнування загальнотеоретичної конструкції. Таким чином, властивості доказів виступають методологічним зв'язком між абстрактною теорією доказування та аналізом конкретних доказових форм у кримінальному процесі.

Перехід від аналізу властивостей доказів до проблеми їх класифікації є логічно зумовленим, оскільки саме через класифікацію відбувається подальша конкретизація теоретичних положень і їх адаптація до потреб правозастосування. Класифікаційні підходи дозволяють впорядкувати різноманіття доказів, виявити їх спільні та відмінні риси, а також уточнити способи реалізації властивостей доказів залежно від їх виду, що зумовлює необхідність звернення до доктринальних підходів до класифікації доказів у кримінальному процесі.

У вітчизняній доктрині кримінального процесу питання класифікації доказів традиційно розглядається як важливий інструмент наукового пізнання та впорядкування доказового матеріалу. Загальновизнаною у науці є класифікація доказів на обвинувальні й виправдувальні, первинні та похідні, прямі й побічні, яка сприймається більшістю процесуалістів як базова та методологічно обґрунтована. Разом із тим у науковій літературі сформувалися й альтернативні підходи до систематизації доказів. Так, С. С. Алексєєв, В. П. Бож'єв і М. А. Чельцов пропонують доповнити традиційні класифікаційні групи поділом доказів на особисті та речові залежно від механізму їх формування. Розгорнуту багатокритеріальну модель класифікації доказів запропонував В. Я. Дорохов, який здійснює їх поділ за шістьма групами, враховуючи види фактичних даних, процесуальні джерела, характер зв'язку з подією кримінального правопорушення, походження доказової інформації, структуру обґрунтування та спрямованість доказування. Водночас у доктрині висловлюється критика окремих класифікаційних критеріїв. Зокрема, М. М. Видря та М. С. Строгович заперечують доцільність поділу доказів на особисті й речові, вбачаючи в ньому штучне протиставлення речових доказів показанням учасників кримінального провадження. Натомість О. О. Хмиров обґрунтовує інший підхід, відповідно до якого такий поділ не має оціночного характеру, а лише відображає об'єктивні відмінності між повідомленнями про факти, що походять від осіб, і матеріальними об'єктами, які потребують специфічного процесуального режиму збирання та закріплення. Окреме місце в науковій дискусії посідає класифікація доказів, запропонована В. П. Гмирком, який розподіляє їх за шістьма групами, використовуючи як критерії походження доказів, їх змістовні та процесуальні

властивості, а також стадію кримінального провадження, в межах якої вони використовуються. Запропонований підхід був підданий частковій критиці з боку С. М. Стахівського, який обґрунтовано заперечує доцільність класифікації доказів за критеріями їх оцінки, зокрема належності, допустимості та достовірності, вважаючи їх не видами доказів, а універсальними властивостями доказового матеріалу. Загалом у наукових працях підкреслюється умовний характер будь-якої класифікації доказів, оскільки віднесення конкретного доказу до тієї чи іншої групи залежить від фактичних обставин кримінального провадження та процесуальної позиції суб'єктів доказування. У цьому контексті увагу привертають підходи, що ґрунтуються на таких критеріях, як відношення доказу до предмета доказування, джерело його отримання та механізм формування. Найбільш зваженою та методологічно вивіреною у вітчизняній доктрині видається класифікація доказів, запропонована С. М. Стахівським, який обмежує їх поділ чотирма групами: первинні та похідні; обвинувальні та виправдувальні; прямі й побічні; особисті та докази, що містяться в об'єктах матеріального світу — предметах і документах. Такий підхід дозволяє уникнути змішування класифікаційних критеріїв із властивостями доказів та зберегти логічну чіткість і прикладну цінність класифікації в механізмі кримінального процесуального доказування [141, с. 26-27].

На нашу думку, класифікація доказів у кримінальному процесі виконує насамперед упорядковувальну та евристичну функції: вона систематизує різноманіття доказового матеріалу, сприяє добору адекватних прийомів його збирання, перевірки й оцінки та полегшує процесуальне планування доказування (підходи до класифікації доказів у контексті можливості їх існування в електронній формі проаналізовано в підрозділі 1.3). Водночас властивості доказів (належність, допустимість, достовірність, достатність) є універсальними правовими критеріями, що визначають якість і процесуальну придатність як окремого доказу, так і доказової сукупності. Отже, класифікація і властивості перебувають у відносинах не конкуренції, а взаємодоповнення: класифікація відповідає на питання «який це доказ» (за джерелом, походженням, спрямованістю, структурою доведення тощо), тоді як властивості — «чи може він бути використаний» і «якою мірою він

переконливий» у межах предмета доказування. Методологічно важливо підкреслити, що класифікаційні поділи не повинні підміняти собою оцінні критерії. Класифікація є інструментом організації доказового матеріалу, тоді як властивості — інструментом його юридичної верифікації й процесуальної легітимації.

Вважаємо, що для забезпечення понятійної визначеності доцільно розмежовувати властивості доказів і суміжні категорії — ознаки, характеристики, параметри. Властивості у кримінальному процесуальному розумінні є юридично значущими і такими, що необхідно оцінюються при вирішенні питання про можливість використання доказу та про обґрунтованість процесуальних рішень. Саме тому належність і допустимість доцільно розглядати як базові властивості, що характеризують, відповідно, змістовну релевантність доказу предмету доказування та його формально-процесуальну легітимність. Достовірність має оціночний характер і виявляється через перевірку та співставлення доказів, а достатність відображає інтегративну якість сукупності доказів.

Натомість, ознаки доцільно вживати для позначення типових рис певного виду доказів (наприклад, для документів, речових доказів, показань чи висновків експерта), що дозволяють їх ідентифікувати або відмежувати, але не визначають автоматично їх процесуальну придатність. Характеристики та параметри здебільшого описують технічні, інформаційні або організаційні особливості фіксації та зберігання відомостей (формат, носій, спосіб створення, метадані, цілісність, відтворюваність, канали передачі тощо). Вони можуть мати суттєве значення для оцінки доказу, але їх правове значення проявляється опосередковано — через вплив на встановлення належності, допустимості, достовірності або достатності.

Розмежування властивостей доказів і їх технічних, або ж інформаційних характеристик, має принципове методологічне значення для уникнення технократичної редукції доказування, за якої доказ ототожнюється з технологічним артефактом або з окремими технічними параметрами носія інформації. Така редукція особливо ризикована у сфері цифровізації, де формальні атрибути (формат файлу, спосіб копіювання, наявність чи відсутність метаданих, тип підпису, геш-сума, лог-файли тощо) можуть помилково сприйматися як самодостатній критерій

оцінки доказу. Насправді ж ці елементи мають юридичне значення настільки, наскільки вони забезпечують або, навпаки, підривають виконання універсальних властивостей доказу. Відтак, в цьому контексті, в межах даного дисертаційного дослідження та з урахуванням його предмету, доцільно приділити особливу увагу таким властивостям доказів як допустимість та, частково, достовірність, що мають пряму кореляцію з технічними характеристиками доказів електронної форми.

На нашу думку, в контексті доказів електронної форми технологічний елемент і технічні характеристики мають розглядатися не як самостійні (нові) властивості доказу, а як релевантні чинники, що впливають передусім на допустимість через дотримання належної правової процедури отримання, фіксації, збереження та подання а також можливість перевірки цілісності, автентичності, незмінності та (або) походження відомостей. Саме таке методологічне позиціонування дозволяє поєднати вимоги кримінального процесуального права із сучасними технологічними реаліями без руйнування загальнотеоретичної конструкції доказування. Відповідні аргументи та прикладні критерії будуть послідовно обґрунтовані у наступних підрозділах дослідження.

Здійснений аналіз вітчизняних доктринальних підходів до розуміння доказів, їх властивостей і класифікації дозволяє сформулювати узагальнюючі положення, необхідні для подальшого, спеціалізованого дослідження доказів електронної форми. Йдеться про такі результати, які одночасно забезпечують спадкоємність із загальною теорією доказування і створюють методологічні межі для коректного розгляду цифрових трансформацій доказової діяльності.

Диференціація доказів у кримінальному процесі має доктринально обґрунтовуватися не довільним множенням їх різновидів, а стійкими юридично значущими критеріями: процесуальними джерелами, механізмом формування доказової інформації, логікою доведення та функціональною роллю доказу у встановленні обставин предмета доказування.

З урахуванням сучасної доктрини кримінального процесу [202], на нашу думку, будь-який вид доказів у кримінальному процесі, незалежно від його процесуального джерела та способу фіксації, є підпорядкованим універсальним

властивостям — належності, допустимості, достовірності й достатності. Ці властивості унеможливають нормативно та методологічно необґрунтовану автономізацію окремих різновидів доказів. При цьому відмінності між видами доказів не скасовують, а лише конкретизують способи досягнення й перевірки їх універсальних властивостей.

З огляду на це, позиція автора полягає в тому, що докази електронної форми на сьогодні не варто виокремлювати як окремий вид доказів у системі кримінального процесу України, оскільки електронна форма представлення є характеристикою існування й подання фактичних даних у межах уже визначених чотирьох видів (процесуальних джерел) доказів (визначених в ч. 2 ст. 84 КПК України). Відповідно, належні правила роботи з носіями інформації, метаданими, підтвердження цілісності даних та іншу технічні характеристики повинні розглядатися як елементи забезпечення таких властивості доказів як допустимість та достовірність, що буде предметно доведено в наступних підрозділах дисертації.

Концептуальна єдність дисертації забезпечується послідовним підпорядкуванням спеціальних питань, пов'язаних із доказами електронної форми, загальнотеоретичним засадам доказування: легальній конструкції доказів і процесуальних джерел, властивостям доказів та доктринально вивіреном підходам до їх класифікації. Методологічні межі аналізу полягають у відмові від технократичного ототожнення доказу з цифровим об'єктом або його параметрами та у збереженні фокусу на кримінальній процесуальній природі доказу як юридично легітимованої інформації, перевіреної й оціненої у контексті процедур, що гарантують забезпечення прав і свободи людини та обґрунтованість процесуальних рішень.

1.2. Концептуальні підходи до доказів електронної форми у кримінальному процесі України

Системна цифрова трансформація кримінальної процесуальної діяльності в Україні протягом останніх років є актуальною тенденцією, обумовленою стрімким розвитком цифрових технологій, характерним для сучасної інформаційної ери. Вже впроваджено значну кількість цифрових інструментів, численні «паперові» процесуальні процедури переведено в електронну форму, що має очевидні позитивні наслідки для практики. Однак така трансформація відбувається не системно. Вказане актуалізує потребу в розумінні та чіткому розмежуванні категорій, що формують електронну (цифрову) складову кримінального процесу України, а також визначенні базових понять досліджуваної сфери.

Метою цього підрозділу є окреслення концептуальних положень електронної (цифрової) складової кримінального процесу України та постановка термінологічного апарату в частині доказів електронної форми у кримінальному процесі України. Це створить теоретичний фундамент для проведення подальшого коректного та термінологічно несуперечливого дослідження. У цьому контексті актуальною і первинною є потреба визначення та структурування елементів, що формують електронну (цифрову) складову кримінального процесу в Україні. Їх чітке окреслення й розмежування має важливе значення як для формування ефективного механізму нормативного регулювання, так і для науки й практики правозастосування, оскільки дозволяє уникнути підміни понять, термінологічної плутанини та забезпечує логічність і послідовність у правозастосуванні.

Сьогодні можна виокремити такі компоненти електронної (цифрової) складової кримінального процесу України: електронне кримінальне провадження; оцифрування матеріалів кримінальних проваджень та їх резервне зберігання; докази електронної форми (електронні (цифрові) докази); електронні інструменти доказування; електронні інструменти реалізації повноважень суб'єктів правозастосування. Чітке окреслення наведених компонентів має важливе

значення як для науки кримінального процесу, так і для практики правозастосування, адже є передумовою їх ефективного розвитку [123, с. 229].

Електронне кримінальне провадження нормативно врегульовано ст. 106-1 КПК України. В науці питанню електронного кримінального провадження присвячені дисертаційні дослідження А. В. Столітнього (2018) [258] та авторки (2017) [120]. Електронне кримінальне провадження, на нашу думку [93; 95], реалізовано в електронній системі управління кримінальними провадженнями щодо корупційних правопорушень e-Case Management System (далі – e-Case) [22] та частково в Єдиному реєстрі досудових розслідувань (далі – ЄРДР) [123, с. 229–230].

Оцифрування матеріалів кримінальних проваджень та їх резервне зберігання наразі врегульовано через призму ч. 14 ст. 615 КПК України. Відповідними положеннями визначено, що копії матеріалів кримінальних проваджень, досудове розслідування в яких здійснюється в умовах воєнного стану, в обов'язковому порядку зберігаються в електронній формі у дізнавача, слідчого чи прокурора. Однак через систематичні обстріли населених пунктів і цивільних об'єктів в Україні існує постійна загроза безповоротної втрати таких матеріалів або навіть носіїв їх електронних копій. З огляду на це рішенням міжвідомчої робочої групи (Координаційного штабу) з питань взаємодії правоохоронних та інших державних органів під час фіксації та розслідування воєнних злочинів і ведення військово-політичним керівництвом Російської Федерації агресивної війни проти України централізованим місцем збереження оцифрованих копій матеріалів кримінальних проваджень для Офісу Генерального прокурора (далі – ОГП), Служби безпеки України (далі – СБУ) та Національної поліції України визначено сховище ОГП, резервними – сховища СБУ та Національної поліції України. Оцифрування матеріалів кримінальних проваджень та їх резервне зберігання не слід ототожнювати з електронним кримінальним провадженням, що часто зустрічається під час дискусій з практичними працівниками [123, с. 230].

Докази електронної форми (електронні (цифрові) докази), є наслідком розвитку цифрових технологій, розповсюдження технічних пристроїв та міграції

злочинності в кіберпростір. Наразі докази електронної форми не визначено в ч. 2 ст. 84 КПК України самостійним процесуальним джерелом доказів, однак деякі законодавчі зміни та практика правозастосування інтегрували їх в наявну концепцію доказів. Їх існування чи не в кожному кримінальному провадженні неможливо ігнорувати [123, с. 230]. Тут варто звернути увагу на дослідження А. В. Скрипника [249], А. В. Гутник (Ратнової) [240; 156], О. П. Метелева [168; 169; 171], І. В. Гори, В. А. Колесника, (2024) [86], а також доробки інших науковців.

Електронні інструменти доказування, на нашу думку, необхідно визначити як сукупність програмних і технічних засобів, а також технічних пристроїв, що застосовуються дізнавачем, слідчим, детективом, спеціалістом, експертом, прокурором, адвокатом, суддею та іншими суб'єктами правозастосування під час виявлення, фіксації, зберігання, опрацювання та дослідження доказів під час кримінального провадження. До цієї категорії доцільно віднести всі програмні та технічні інструменти цифрової криміналістики та програмні й технічні засоби, що застосовуються, наприклад, під час проведення експертизи комп'ютерної техніки й програмних продуктів. Одним з яскравих та корисних прикладів такого спеціалізованого інструменту є Cellebrite UFED (програмно-апаратний комплекс для вилучення та аналізу даних із мобільних пристроїв, розроблений компанією Cellebrite) [123, с. 231]. Цікавим цьому контексті є дослідження Ю. П. Поляка (2022) [215], а також Національної академії СБУ (2025) [153] та Національного юридичного університету імені Ярослава Мудрого (2025) [37].

Електронні інструменти реалізації повноважень суб'єктів правозастосування необхідно розглядати в контексті інструментів кримінального процесу – визначених кримінальним процесуальним законом спеціалізованих правореалізаційних засобів, що забезпечують здійснення кримінальних процесуальних процедур; створення, збирання, зберігання, захист, облік та використання процесуальної інформації; взаємодію суб'єктів провадження та здійснення процесуального контролю [123, с. 231]. Інструменти (правореалізаційні засоби) поділяються на: а) інструменти, призначені для паперових форм фіксації: папір, засоби письма, персональний комп'ютер, текстовий редактор, принтер;

б) інструменти електронної та змішаної форм фіксації провадження: 1) інформаційно-комунікативні пристрої («залізо»); 2) носії інформації; 3) програмне забезпечення (далі – ПЗ): загальнонавчальне: Word, Word Perfect, Excel, електронна пошта тощо; і спеціалізоване – призначене для виконання завдань кримінального процесу (ЄРДР, Єдиний державний реєстр судових рішень, Єдина судова інформаційно-комунікаційна система, e-Case тощо). Окремим елементом цієї групи вважаємо забезпечення доступу суб'єктів правозастосування до мережі Інтернет [123, с. 231].

Ці п'ять компонентів електронної (цифрової) складової кримінального процесу України належать до сфери наукових досліджень кримінального процесу та криміналістики (12.00.09). Досить часто наукові дослідження вчених відповідної спеціалізації охоплюють одразу кілька з них. Однак часом указані компоненти відображено в наукових роботах доволі хаотично, відповідні компоненти не розмежовуються (через не усвідомлення їх природи та специфіки), а поняття підміняються й хибно трактуються.

Приміром, у низці досліджень спостерігається некоректне узагальнення сутнісно різних компонентів, що співвідносяться між собою лише номінально або поверхово. Трапляються випадки, коли ототожнюються, наприклад, «електронне кримінальне провадження» та «докази електронної форми», які виконують різні процесуальні або технічні функції. На жаль, подібні випадки трапляються все частіше. Не менш проблемним є їх сприйняття суб'єктами правозастосування, що ототожнюють або підміняють окремі компоненти. Тому сепарація наведених нами компонентів електронної (цифрової) складової кримінального процесу України заслуговує на особливу увагу, однак потребує глибокого розуміння їх правової природи й особливостей практичного застосування.

Нерозуміння багаторівневої природи електронної (цифрової) складової кримінального провадження у сфері доказів та доказування, на нашу думку, є прямим наслідком одночасної дії двох чинників: по-перше, наявності в науці кримінального процесу значної кількості розрізнених підходів і моделей, що

конкурують між собою за концептуальний статус; по-друге, неналежне нормативне регулювання у КПК України інституту «електронних» або ж «цифрових» доказів.

З огляду на окреслене вище, спробуємо подолати зазначену концептуальну невизначеність шляхом застосування комплексного підходу до дослідження доказів електронної форми у кримінальному процесі України. Це дослідження передбачає формування цілісного уявлення про сутність, класифікацію та функціональне призначення такої форми доказів, а також обґрунтування механізму їх нормативної імплементації у чинну модель кримінального процесуального регулювання. Пропонований підхід дозволяє вийти за межі прикладного сприйняття окремих процесуальних дій і розглядати докази електронної форми як системну категорію, інтегровану в усі ключові елементи доказування.

Нормативною основою використання доказів електронної форми у кримінальному процесі України, виступають такі джерела законодавчого регулювання у цій сфері: КПК України [155, с. 1]; Конвенція про кіберзлочинність від 23 листопада 2001 року, ратифікована Законом України від 7 вересня 2005 року № 2824-IV (далі – Конвенція про кіберзлочинність) [148, с. 1]; Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV (далі – Закон України «Про електронні документи та електронний документообіг») [225, с. 1]; Закон України «Про електронну ідентифікацію та електронні довірчі послуги» від 5 жовтня 2017 року № 2155-VIII (далі – Закон України «Про електронну ідентифікацію та електронні довірчі послуги») [227, с. 1]; Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР [230, с. 1]; Практика Європейського суду з прав людини (далі – ЄСПЛ) [113; 117; 121; 327-346]; Практика Верховного суду (далі – ВС) [15]; ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» доказів (далі – ДСТУ ISO/IEC 27037:2017) [83]; Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних (далі – Протокол Берклі) [238; 318].

У ст. 96 Господарського процесуального кодексу України (далі – ГПК України), ст. 99 Кодексу адміністративного судочинства України (далі – КАС України), ст. 100 Цивільного процесуального кодексу України (далі – ЦПК України) законодавець закріпив єдину позицію та визначив, що електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (у тому числі в мережі Інтернет) [260, с. 183].

Р. І. Благута та А. В. Мовчан (2020) вказують, що на відміну від ЦПК України, ГПК України та КАС України, КПК України й Кодекс України про адміністративні правопорушення інституту електронних доказів не отримали. Такий вибірковий підхід викликає подив у науковців і практиків з огляду на наявність у Кримінальному кодексі України (далі – КК України) розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», а також відповідальності за незаконні дії з електронними грошима (ст. 200 КК України) або за шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ст. 190 КК України) [24, с. 111–112].

Однак необхідно чітко визначити, що нормативні положення, які стосуються електронних доказів і передбачені ст. 100 ЦПК України, ст. 96 ГПК України та ст. 99 КАС України, не можуть бути застосовані в кримінальному процесі з огляду на низку доктринальних, системно-правових і процесуальних аргументів, зокрема:

1) принцип процесуальної автономії. Кожен процесуальний кодекс України побудований на основі окремих принципів, логіки та процедур, що відповідають природі відповідного виду судочинства. Кримінальний процес, на відміну від

цивільного, господарського чи адміністративного, має публічно-правовий характер, зумовлений необхідністю переслідування за кримінальні правопорушення та спеціальні вимоги до допустимості доказів. У зв'язку з цим положення інших процесуальних кодексів не можуть автоматично переноситися в кримінальне провадження, що має специфічну модель доказування;

2) відсутність законодавчих відсилань у КПК України. КПК України не містить бланкетних норм до відповідних статей некримінальних процесуальних кодексів, а отже, немає правової підстави для їх прямого застосування у кримінальному процесі згідно з ч. 3 ст. 9 КПК України;

3) різна правова природа доказів у різних видах судочинства. У кримінальному процесі доказами визнаються лише ті фактичні дані, які отримані у порядку, визначеному КПК України. У інших видах судочинства діє принцип диспозитивності, що допускає гнучкість в оцінці доказів, зокрема й електронних. Тому підходи, прийнятні у межах приватноправового спору, не забезпечують належного рівня процесуальних гарантій у кримінальному провадженні, де діє суворіший стандарт допустимості доказів;

4) ризик порушення принципу законності. Застосування положень інших кодексів без належної імплементації до структури кримінального процесу створює ризик визнання доказу недопустимим через порушення вимог до його форми, джерела чи способу одержання. Така практика прямо суперечить принципу законності (ч. 1 ст. 9 КПК України), згідно з яким під час кримінального провадження повинні дотримуватись вимоги саме КПК України.

5) потреба у спеціальному правовому режимі. Кримінальне судочинство вимагає створення власної, спеціальної регламентації обігу, подання, дослідження та перевірки доказів, що враховує специфіку слідчих (розшукових) дій, негласних слідчих (розшукових) дій (далі – НСРД), роботи експертів тощо. Запозичення норм інших кодексів не вирішує цієї проблеми, а навпаки – ускладнює її.

Таким чином, положення ЦПК України, ГПК України та КАС України, що регламентують обіг електронних доказів у відповідних юрисдикціях, не можуть бути застосовані в кримінальному процесі ні прямо, ні за аналогією, оскільки

суперечать базовим принципам кримінального процесу, не відповідають його доказовій системі, не мають нормативної прив'язки в КПК України і можуть призвести до порушення засад кримінального провадження.

На нашу думку, така досить прискіплива увага до норм некримінальних процесуальних кодексів України в контексті досліджуваної теми є виправданою та необхідною з огляду на значну увагу до них науковців, що супроводжується спробами їх використання при формуванні підходів для кримінального процесу щодо роботи з доказами електронної форми. Також спостерігаються непоодинокі спроби представників сторони захисту трактувати досліджувану форму доказів під час кримінального провадження через призму норм саме ЦПК України, ГПК України та КАС України. Тому в цій частині необхідно внести ясність й акцентувати на неможливість застосування відповідних норм у кримінальному процесі України.

Необхідність чіткого визначення і розмежування термінів не є новою для юридичної науки. У досліджуваній сфері це особливо актуально з огляду на прогалини нормативного регулювання та значну кількість наукових праць, що сформували різні підходи, зокрема й термінологічні. Цікавою спробою такої термінологічної розвідки є дослідження А. В. Скрипника (2021) [249, с. 67–95], аналізуючи десятки суміжним понять, застосованих в КПК України [249, с. 67-68].

На нашу думку, така ситуація виникла внаслідок того, що при внесенні численних змін до КПК України законотворці зосереджувалися переважно на процесуальних, а не на технічних аспектах правового регулювання. Щоб не створювати загроз для стабільності практики правозастосування, пов'язаних із заміною технічних термінів, законодавець здебільшого залишав усталені формулювання, а нові — додавав поряд, через кому. Такий підхід, очевидно, обумовлювався тим, що на момент внесення змін тривало досудове розслідування у великій кількості кримінальних проваджень, у межах яких в ухвалях слідчих суддів про надання дозволу на проведення обшуку, проведення НСРД, арешт майна, численних протоколах слідчих (розшукових) дій, а також постановках про визнання речовими доказами використовувалась чинна на той момент термінологія

КПК України. Її заміна могла б спричинити ризики визнання відповідних доказів недопустимими у зв'язку з формальними запереченнями сторони захисту, пов'язаними з відмінністю у назві чи формулюванні терміна. Безумовно, сторона захисту вільна у виборі тактики захисту та має право використовувати будь-які допустимі засоби, що відповідає змагальному характеру кримінального процесу. Однак масштабна хвиля формалізованих клопотань щодо недопустимості доказів на цій підставі вбачається небажаною з позиції стабільності кримінального провадження. Володіючи десятирічним досвідом правозастосовника, ми вважаємо такий обережний підхід законодавця раціональним і зваженим у контексті забезпечення процесуальної безперервності. Проте з наукового погляду така ситуація призводить до надмірного накопичення синонімічних або функціонально дублюючих понять, що створює термінологічну надмірність і знижує рівень системності законодавства. Така «гібридна» модель законодавчого регулювання може бути виправданою з погляду поточної правозастосовної практики, але вимагає подальшого доктринального переосмислення та уніфікації у довгостроковій перспективі.

Виділимо основні категорії, які існують у законодавстві та які важливі в межах цього дослідження і використовуватимуться нами в роботі.

Розмежування понять «письмовий» і «паперовий» у контексті кримінального процесуального документування має фундаментальне значення для правильного розуміння форм фіксації процесуальної інформації. Не слід ототожнювати письмову форму фіксації кримінального провадження з паперовим документом. Так, академічний тлумачний словник української мови визначає термін «письмовий» як: 1. виражений графічними знаками; написаний; 2. який служить або вживається для писання [5, с. 1]. Тож письмова форма фіксації інформації залежить від способу її вираження у формі графічних знаків, а не від матеріалу, на якому такі графічні знаки зафіксовано. Це означає, що ключовим критерієм визначення письмового документа є не носій (паперовий чи електронний), а спосіб фіксації його змісту. Такий підхід відповідає сутнісним характеристикам письмової форми, яка є способом надання значущості інформації шляхом її візуалізації за

допомогою письмових знаків. Отже, текстовий документ є письмовим документом, незалежно від форми носія (паперовий чи електронний).

Розмежування категорій «джерела доказів у розумінні ст. 84, ст. 99 КПК України», якими є процесуальні джерела доказів у кримінальному провадженні, та «джерела доказів (загалом)» як всі можливі види й форми вираження інформації, що існують в реальній дійсності та які можуть містити відомості, що мають значення для кримінального провадження. Потрібно чітко диференціювати категорії «джерела доказів у розумінні ст. 84, ст. 99 КПК України» та «джерела доказів (загалом)», оскільки йдеться про два різних рівні аналізу доказової інформації — нормативно-процесуальний і фактико-онтологічний. У вузькому процесуальному розумінні, визначеному ч. 2 ст. 84 КПК України, джерела доказів становлять вичерпний перелік форм процесуального закріплення фактичних даних, які можуть бути використані як докази в кримінальному провадженні: показання, речові докази, документи, висновки експертів. Цей перелік виконує функцію процесуального фільтра допустимості доказів — лише ті відомості, що набули форми, передбаченої законодавством, визнаються джерелами доказів, які можуть бути використані в кримінальному провадженні. У широкому, доктринальному розумінні термін «джерела доказів» охоплює будь-які об'єкти, явища чи інформаційні конструкції, що у своєму змісті містять або можуть містити відомості, що мають значення для встановлення обставин кримінального провадження. Це — онтологічна категорія, яка не зводиться до процесуального оформлення, а відображає первинну природу походження інформації. Наприклад, слід на цифровому носії, файл журналу подій, цифрове зображення чи голосове повідомлення, незалежно від того, чи оформлені вони належним чином, уже потенційно містять доказову інформацію.

Не врахування цієї дихотомії призводить до концептуальної плутанини між носієм фактичних даних і формою його допустимого використання в кримінальному процесі. Тому, з наукового та прикладного поглядів, важливо розмежовувати ці поняття: «джерело доказу загалом» — це об'єкт або носій

фактичних даних; «процесуальне джерело доказу» — це результат належного процесуального оформлення такого об'єкта відповідно до вимог КПК України.

Розмежування категорій «документ як джерело доказів у розумінні ст. 84, ст. 99 КПК України», «документ у розумінні законодавства» та «документ у побутовому розумінні аркуша паперу (або файлу Word) з певною інформацією». У кримінальному процесі України документ як джерело доказів має чітке правове значення, закріплене в ч. 2 ст. 84 КПК України, його визначення деталізовано в ч. 1 ст. 99 КПК України, а у ч. 2 цієї статті подано перелік об'єктів, що можуть вважатися документами в цьому розумінні. Такий документ повинен відповідати вимогам належності, допустимості та містити фактичні дані, що мають значення для встановлення обставин кримінального правопорушення. Натомість у непрофільному законодавстві, наприклад у ст. 1 Закону України «Про інформацію» наведено визначення документа як матеріального носія, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі [232, с. 1]. При цьому визначення складових чи обов'язкових реквізитів документа цей Закон не містить.

У ч. 2 ст. 9 Закону України «Про бухгалтерський облік та фінансову звітність в Україні» визначено обов'язкові реквізити первинних документів, що можуть бути складені у паперовій або в електронній формі [222, с. 1].

Постанова Кабінету Міністрів України «Деякі питання документування управлінської діяльності» від 17 січня 2018 р. № 55 затверджує Типову інструкцію з діловодства в міністерствах, інших центральних та місцевих органах виконавчої влади, яка встановлює єдині вимоги до складання, оформлення, реєстрації та зберігання документів. У п. 15 вказаної Типової інструкції визначено обов'язкові для певного виду документа реквізити, що він їх повинен містити та що розміщуються в установленому порядку [69, с. 1].

ДСТУ 4163:2020 «Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів» визначає склад реквізитів документів; вимоги до змісту та місця розташування реквізитів у документах; вимоги до бланків та оформлення документів; вимоги до їх виготовлення [78].

Згідно з приміткою до ст. 358 КК України під офіційним документом у цій статті та статтях 357, 366 цього Кодексу слід розуміти документи, що містять зафіксовану на будь-яких матеріальних носіях інформацію, яка підтверджує чи посвідчує певні події, явища або факти, які спричинили чи здатні спричинити наслідки правового характеру, чи може бути використана як документи — докази у правозастосовній діяльності, що складаються, видаються чи посвідчуються повноважними (компетентними) особами органів державної влади, місцевого самоврядування, об'єднань громадян, юридичних осіб незалежно від форми власності та організаційно-правової форми, а також окремими громадянами, у тому числі самозайнятими особами, яким законом надано право у зв'язку з їх професійною чи службовою діяльністю складати, видавати чи посвідчувати певні види документів, що складені з дотриманням визначених законом форм та містять передбачені законом реквізити [154, с. 1].

Усе це уможливлює ситуацію, за якої один і той самий електронний файл, визнаний документом в законодавстві (законах, постановах Кабінету Міністрів України тощо), не буде автоматично вважатися процесуальним джерелом доказів без відповідної правової оцінки за критеріями КПК України.

Документ у побутовому розумінні зазвичай асоціюється із будь-яким аркушем паперу або цифровим файлом (наприклад, документом Word або PDF), що містить текстову або графічну інформацію. Така форма розуміння документа є не фаховою, не враховує юридичного змісту поняття і не містить посилань на його процесуальний статус, способи отримання, автентифікацію чи правові наслідки використання.

Таким чином, ототожнення наведених категорій є хибним як з позиції юридичної техніки, так і практики правозастосування, однак спостерігається досить часто. Відсутність чіткої диференціації між ними ускладнює правову оцінку доказів і може призвести до їх неправильного тлумачення. Саме тому чітке розмежування понять «документ» у зазначених контекстах має бути однією з методологічних передумов аналізу доказів в електронній формі.

Отже, розмежування категорій:

- документ у розумінні статей 84, 99 КПК України, який має електронну форму та часто помилково іменується як «електронний документ»;
- електронний документ в розумінні Закону України «Про електронні документи та електронний документообіг», підписаний кваліфікованим електронним підписом (далі – КЕП);
- документ, що має електронну форму, в побутовому розумінні, коли це електронний файл, що має формальну структуру документа та не підписаний КЕП.

А. М. Гаркуша (2024) слушно зауважує, що обґрунтування потреби у диференціації зазначених категорій засноване на доктринальній, техніко-юридичній та процесуальній неоднорідності об'єктів, що позначаються схожими словами, але мають різну правову природу, доказове значення та процесуальний режим. По-перше, документ у розумінні статей 84, 99 КПК України, у тому числі той, що має електронну форму, є одним із процесуальних джерел доказів. Ця категорія має чітко встановлені в КПК України вимоги, отож не кожен файл, що має електронну форму, автоматично набуває статусу такого документа. По-друге, електронний документ у розумінні Закону України «Про електронні документи та електронний документообіг» — це нормативно закріплений у ст. 5 цього Закону термін, що передбачає наявність не лише електронної форми, а й обов'язкових реквізитів, зокрема КЕП чи електронної печатки. Такий документ може бути використаний як доказ у кримінальному процесі, однак його правова природа не збігається повністю з вимогами КПК України до процесуального документа як джерела доказу. Зокрема, електронний документ у розумінні Закону України «Про електронні документи та електронний документообіг» може бути як документом у розумінні ст. 84 КПК України, так і однією з форм висновку експерта, або ж формою протоколу допиту свідка тощо. КПК України не містить автономного визначення терміна «електронний документ», тому за правилами, установленими ч. 3 ст. 3 КПК України, для його визначення слід звернутися до спеціальних норм в інших законах України [43, с. 74] - Закону України «Про електронні документи та електронний документообіг» [225, с. 1] та Закону України «Про електронну ідентифікацію та електронні довірчі послуги» [227, с. 1].

Науковці також визначають і описують ці категорії. Так, О. В. Шведова (2006) вказує, що загальними ознаками, тобто такими, що притаманні кожному електронному документі, є: формат і структура даних, які його складають, наявність (відсутність) певних реквізитів, візуальна форма представлення; окремі ознаки, які можуть існувати в деяких електронних документах: конкретні електронні дані, програмні, програмно-апаратні й апаратні засоби, методи його підготовки, створення, передачі, перевірки цілісності; параметр криптографічного алгоритму формування електронного підпису, який відомий лише конкретній особі [290, с. 14]. Д. О. Алексєєва-Процюк, О. М. Брисковська (2017) загальними ознаками електронних документів називають таке: існують у нематеріальному вигляді; створюються людиною, або комп'ютерною системою; не можуть існувати поза межами фізичного носія або каналу зв'язку; не мають нерозривного зв'язку з матеріальним носієм; вільно переміщуються в електронній мережі; сприйняття та дослідження таких документів може здійснюватися лише з використанням спеціальних програм та пристроїв; потребують спеціального порядку збирання, перевірки й оцінки; мають здатність до дубляжу, тобто копіювання або переміщення на інший носій без втрати своїх характеристик; можливість дистанційного внесення змін до них та їх знищення [7, с. 252]. При цьому вчені не акцентують саме на наявності КЕП, що залишає нам лише здогадуватися зі змісту наукової публікації, в якому саме розумінні та контексті вживається відповідний термін. А. В. Гутник (Ратнова) (2017) слушно зазначає, що використання законодавчо закріпленого у Законі України «Про електронні документи та електронний документообіг» визначення електронного документа неможливе у кримінальній процесуальній діяльності. Електронному документу притаманна наявність певних реквізитів, проте вона не є обов'язковою для усіх них. У порядку здійснення цивільно-правових відносин деякі правочини визнаються недійсними й не мають юридичної сили без таких обов'язкових реквізитів документа (дата складання, сторони та умови угоди, електронний підпис). Проте всі інші електронні документи існують без основних реквізитів й можуть бути використані як джерело доказу [239, с. 91].

Ми вважаємо доцільним для завдань кримінального провадження називати згадану категорію все ж не «електронний документ», а радше «документ електронної форми»; і хоча така конструкція більш громіздка, однак є несутеречливою термінологічно.

По-третє, документи, що мають електронну форму, в загальному розумінні — це найширша категорія, що охоплює будь-які файли у форматі .pdf, .doc, .jpg тощо, що містять інформацію і мають зовнішні ознаки документа (заголовок, підпис, дата тощо), але не підписані електронним підписом і не відповідають вимогам ані КПК України, ані Закону України «Про електронні документи та електронний документообіг». Такі файли, хоча й можуть мати певну інформативну цінність, самі по собі не забезпечують належного рівня автентичності, не завжди відповідають вимогам до документів як джерел доказів у кримінальному процесі та потребують додаткової перевірки, процесуального підтвердження й оформлення. Наприклад, цю категорію визначено в ДСТУ 7157:2010 «Інформація та документація. Видання електронні. Основні види та вихідні відомості» як електронний документ – документ, інформація, в якому подана у формі електронних даних і для використання якого потрібні засоби обчислювальної техніки [79, с. 2]. Так само у наказі Міністерства освіти і науки, молоді та спорту України від 1 жовтня 2012 року «Про затвердження Положення про електронні освітні ресурси» № 1060 визначено електронний документ як документ, інформація в якому подана у формі електронних даних і для використання якого потрібні технічні засоби [214, с. 1].

Як бачимо, ототожнення вказаних категорій спричиняє плутанину при аналізі їх допустимості, дослідженні порядку їх фіксації, збирання, перевірки та використання під час кримінального провадження.

Співвідношення категорій «носії інформації»/«електронні носії інформації» (у контексті п. 3 ч. 2 ст. 99 КПК України), «комп'ютерні дані» (у контексті п. 1 ч. 2 ст. 99 КПК України) та «електронний документ» (в контексті ст. 5 Закону України «Про електронні документи та електронний документообіг»). У контексті кримінального процесу категорії «носії інформації» / «електронні носії

інформації», «комп'ютерні дані» та «електронний документ» співвідносяться між собою як такі, що утворюють ієрархічну структуру від загального до часткового. Найширшим поняттям у цій системі є «носії інформації» (п. 3 ч. 2 ст. 99 КПК України) та їх підкатегорія – «електронні носії інформації», які охоплюють будь-які засоби цифрової техніки, технічні засоби чи машинні носії, призначені для фіксації й збереження цифрових даних. У межах цього поняття виокремлюються «комп'ютерні дані» (п. 1 ч. 2 ст. 99 КПК України) як специфічна форма збереженої інформації у цифровому вигляді. Релевантне визначення наведено в ст. 1 Конвенції про кіберзлочинність, що визначає в п. «b» ст. 1 комп'ютерні дані як будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою [148, с. 1].

Ще вужче поняття – «електронний документ» (у розумінні ст. 5 Закону України «Про електронні документи та електронний документообіг»), який становить юридично значущу форму відображення комп'ютерних даних. Таким чином, електронний документ є формалізованим різновидом комп'ютерних даних, що зберігається на електронному носії інформації.

Розмежування категорій «електронний» та «цифровий». У процесі дослідження сучасної наукової доктрини, а також аналізу правозастосовної практики впадає в око термінологічна невизначеність, що виникає через паралельне використання понять «електронний доказ» та «цифровий доказ» як ніби тотожних. Така тенденція спостерігається як у наукових працях, так і у публічній комунікації правоохоронних органів та судових установ. Утім, з точки зору правової і технічної природи цих понять, їх ототожнення – хибне й призводить до розмиття меж між різними за сутністю явищами [122, с. 195].

Термін «цифровий» (від англ. digital) відображає інформаційно-змістовну характеристику об'єкта, вказуючи на те, що дані подані у вигляді дискретного, числового (бінарного) коду. У кримінальному процесі мова йде передусім про цифрові сліди, метадані, файли, записи та інші дані, що є носіями змісту, який має доказове значення. Тобто цифровий вимір доказу — це передусім інформація, яка

внаслідок цифровізації здатна до кодування, передачі, копіювання, обробки й зберігання. При цьому носій даних або спосіб їх передачі не є визначальним для класифікації як «цифровий» [122, с. 195–196]. А ось термін «електронний» (від лат. *electronicus*) характеризує форму, середовище або спосіб фіксації й збереження інформації. У правозастосовному контексті йдеться переважно про електронні документи, електронні бази даних, електронні інформаційні системи, що забезпечують існування інформації в електронному вигляді, незалежно від того, чи є її вміст результатом оцифрування або створений безпосередньо у цифровому середовищі [122, с. 196].

Тож терміни «електронний» та «цифровий» не є взаємозамінними, бо позначають різні за природою аспекти одного явища: перший – форму існування, другий – змістову структуру інформації. Наприклад, електронний документ може містити як цифрові, так і не диференційовані за структурою дані; навпаки – цифрові докази можуть бути подані в електронній, змішаній або навіть матеріалізованій формі [122, с. 196].

Розмежування категорій «електронні докази», «докази електронної форми» та «цифрові докази». У пункті 3.5 ДСТУ ISO/IEC 27037:2017 закріплено термін «цифровий доказ (*digital evidence*)», під яким державний стандарт розуміє інформацію або дані, збережені або передані в бінарному вигляді, на які можна покладатися як на докази [83, с. 2].

Поділяємо твердження А. В. Скрипника, що: цифровий доказ — це: а) цифрова інформація, почерпнута шляхом відтворення з використанням технічних засобів змісту файлу, збережуваного на носії цифрових даних (теоретичне визначення); б) цифрова інформація, отримана у передбаченому КПК України порядку, на підставі якої дізнавач, слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню (нормативне визначення) [249, с. 94].

З огляду на викладене вважаємо за необхідне запропонувати робочі дефініції, що відображають підхід, обраний у межах цього дослідження.

Цифровий доказ — це інформація, що існує у вигляді цифрового (переважно бінарного) коду, отримана, збережена або передана за допомогою цифрових технологій, і має значення для встановлення обставин у кримінальному провадженні. Така інформація може зберігатись на електронних носіях, в електронних системах або бути отриманою в результаті оцифрування фізичних об'єктів.

Електронний доказ — це доказ, який існує в електронному середовищі та реалізується за допомогою електронних засобів фіксації, зберігання та обробки інформації. У процесуальному сенсі такий доказ є результатом використання електронних форм документообігу, баз даних, цифрових платформ тощо [122, с. 196]. При цьому варто вказати на пропозиції окремих практиків, котрі відносять до цієї категорії також плівкові аудіозаписи та відеозаписи, адже для їх відтворення необхідні технічні пристрої, що споживають електроенергію. У посібнику «Electronic evidence guide as basic guide for police officers, prosecutors and judges» електронним доказом називають будь-яку інформацію, яка створюється, зберігається або передається у цифровій формі і може бути використана для доведення або спростування факту, який оспорується в судовому процесі [388, с. 12].

Конвенція про кіберзлочинність у п. «с» ч. 2 ст. 14, ст. 23, ч. 1 ст. 25, ч. 1 ст. 35 використовує термін «evidence in electronic form» [513, с. 1], що в офіційному перекладі визначено як «докази в електронній формі» [148, с. 1].

Отже, цифрові докази можуть існувати як у формі електронного документа (в розумінні Закону) чи документа, що має електронну форму, так і поза ним, наприклад, у вигляді метаданих, записів, зафіксованих системами спостереження, цифрових журналів реєстрації тощо. Натомість не кожен електронний документ містить цифрові дані, які мають доказове значення. Така термінологічна диференціація є необхідною передумовою для формування уніфікованої правової позиції щодо використання доказів електронної форми у кримінальному процесі України [122, с. 196].

Аналіз закордонних публікацій та нормативно-правових актів (далі – НПА) свідчить про те, що науковці й практики найчастіше використовують термін «electronic evidence» (з англ. «електронний доказ»), або «digital evidence» (з англ. «цифровий доказ»). Поняття «електронний документ» практично не використовується [240, с. 168]. При цьому для європейського сегменту характерна категорія «electronic evidence», а для американського – «digital evidence», що використовується і в законодавстві, і в наукових дослідженнях і є радше традицією слововживання, адже не простежується їх термінологічна диференціація.

На жаль, термінологічна плутанина ускладнює формування цілісної позиції щодо правової природи відповідних доказів. Особливо це стосується таких термінів, як «цифрові докази», «електронні докази» та «докази електронної форми». З урахуванням як технічного, так і правового їх змісту пропонуємо розмежовувати ці категорії: цифровий доказ – це змістовна інформація, представлена у вигляді цифрового (бінарного) коду, яка може бути збережена, передана або оброблена за допомогою інформаційних технологій (далі – ІТ) і має доказове значення у кримінальному провадженні; електронний доказ – це доказ, що реалізується в електронному середовищі та зберігається за допомогою електронних носіїв або інформаційних систем, незалежно від того, чи має він цифрову структуру. Такий доказ характеризується саме формою фіксації та способом технічної реалізації; доказ електронної форми – це узагальнююче поняття, яке використовується у контексті кримінального процесу для позначення будь-якого доказу, поданого або збереженого в електронному форматі, без зміни його джерела або процесуальної природи [122, с. 196-197].

Таким чином, цифровий доказ відповідає змісту, електронний доказ – технічному способу реалізації, а доказ електронної форми – процесуальній формі подання. Уніфікація цих понять на законодавчому рівні, а також їх чітке методологічне розрізнення в науці кримінального процесу є необхідною умовою ефективної цифрової трансформації правосуддя та побудови сучасної й ефективної системи пошуку, фіксації та використання доказів електронної форми в кримінальному процесі України.

Термінологічна чіткість у розмежуванні понять «електронний доказ», «цифровий доказ» та «доказ в електронній формі» є не просто питанням академічної точності, а необхідною умовою для ефективного функціонування механізмів кримінального процесу в умовах цифровізації. Це дозволяє врахувати як змістовну природу інформації (цифровий доказ), так і технічну форму її існування (електронний доказ), а також процесуальний статус та спосіб подання (доказ електронної форми) [122, с. 197]. У контексті викладеного вище «Мовний коментар до Конституції України та інших нормативних актів» (2025) [173] вбачається дуже вдалим прикладом, який варто поширити на сферу кримінального процесу України.

Ще одним важливим аспектом цього дисертаційного дослідження є методологічний. Нами послідовно використовується авторська методологія [108, с. 56-68], заснована на міждисциплінарних підходах, що релевантна гібридному юридично-технічному предмету цього дисертаційного дослідження.

Проведене в цьому підрозділі дослідження допомагає сформулювати базові концептуальні та термінологічні орієнтири, необхідні для подальшого наукового аналізу доказів електронної форми у кримінальному процесі України. Окреслення електронної (цифрової) складової кримінального провадження як багаторівневої системи з п'яти взаємопов'язаних компонентів дозволяє уникнути поширеної плутанини між категоріями, що мають різну функціональну та нормативну природу. Розмежування понять на основі системного, логічного і техніко-юридичного аналізу забезпечує термінологічну узгодженість дослідження й є передумовою побудови ефективної моделі нормативного регулювання доказів електронної форми у кримінальному процесі України.

1.3. Ретроспектива формування інституту електронних (цифрових) доказів у кримінальному процесі України

Формування інституту електронних (цифрових) доказів у кримінальному процесі України є результатом поступової адаптації правозастосовної та наукової думки до умов цифрової трансформації суспільства, ролі електронної складової у правовій дійсності. Вітчизняна юридична наука послідовно вибудовувала уявлення про докази в електронній формі, про їх місце у структурі кримінального процесу.

У цій частині монографії проведемо ретроспективний аналіз наукових підходів, що сформувались упродовж останніх десятиліть у межах українського кримінального процесуального дискурсу. Тому концептуальні розбіжності між дослідниками та різними науковими школами не розглядаються нами як взаємовиключні чи помилкові, навпаки, вони відображають багатогранність феномену, що перебуває в процесі свого інституційного оформлення. У фокусі аналізу — еволюція термінології, спроби класифікації, співвідношення з традиційними процесуальними категоріями, виокремлення нової категорії доказів, а також пропозиції щодо зміни законодавства. Різноманітність підходів розглядаються в історичному контексті як свідчення поступового усвідомлення унікальності цифрових явищ у сфері доказування та прагнення науки сформулювати реалістичний погляд на цей правовий феномен.

Для зручності сприйняття матеріалу та кращого розуміння еволюції наукової думки під час цитування поглядів учених вказуватимемо рік публікації відповідної праці. Це допоможе читачеві краще орієнтуватися у процесі становлення досліджуваного інституту та співвіднесенні змісту позицій науковців із конкретним етапом розвитку правової доктрини, а також суспільно-політичним контекстом і рівнем розвитку ІТ.

Уже тривалий час українські вчені розглядають різні аспекти інституту електронних (цифрових) доказів у кримінальному процесі України, але й досі спостерігається низка концептуальних неузгодженостей. Тому доцільно розпочати аналіз з огляду основних наукових концепцій, що склалися у вітчизняній

кримінальній процесуальній доктрині щодо місця доказів електронної форми у системі процесуальних їх джерел. Саме ці теоретичні підходи визначають межі дискусії, впливають на вироблення законодавчих моделей та формують методологічні орієнтири для майбутніх досліджень.

Досить поширеною є позиція, згідно з якою докази в електронній формі ототожнюються з уже наявними процесуальними джерелами доказів – переважно з документами або речовими доказами. Одна група вчених відносить докази електронної форми до такого процесуального джерела доказів, як документи. Г. Л. Чигрина (2004) у своїй роботі зазначила, що електронний документ доцільно використовувати як джерело доказу тоді, коли у ньому наявна інформація, яка має значення для правильного вирішення провадження. Вона також пропонує порядок залучення електронного документа до кримінального процесу, який доцільно закріпити у КПК України [287, с.15]. Аналогічну позицію демонструють О. В. Шведова (2006) [290], С. С. Чернявський (2010) [286] та С. Й. Гонгайло (2013) [55], виділяючи електронний документ як різновид документа.

Інша група вчених відносить докази електронної форми до такого процесуального джерела доказів, як речові докази. А. С. Білоусов (2008) пропонує розглядати комп'ютерні об'єкти як один з різновидів окремої групи речових доказів. Вчений вказує, що комп'ютерні об'єкти можна розглядати як один з різновидів окремої групи речових доказів, специфіка яких зумовлена сферою використання з метою створення, обробки, накопичення чи передачі інформації в її електронному вигляді [23, с. 14].

І. О. Крицька (2017) вважає за доцільне визнавати цифрові джерела доказової інформації саме речовими доказами, враховуючи наявність: 1) змісту – самої цифрової інформації, специфічними особливостями якої є її трансльованість (можливість бути переданою з одного носія на інший), мультиплікативність (можливість одночасного існування однієї й тієї ж інформації на різних носіях) та мінливість (можливість бути зміненою з віддаленого доступу або взагалі без участі людини за допомогою спеціально створеної програми); 2) матеріальної форми –

цифрового носія інформації та 3) процесуальної форми – відповідного процесуального оформлення [158, с. 45].

Деякі дослідники визнають за такими об'єктами змішану природу, вважаючи, що залежно від обставин останні можуть бути як документами, так і речовими доказами. С. М. Стахівський (2005) виокремлює електронні речові докази та електронні документи. Він визначає електронні речові докази як будь-які носії комп'ютерної інформації чи програмні об'єкти, які містять специфічні сліди злочину чи інформацію, що буде сприяти встановленню злочину. А електронний документ – це комп'ютерна інформація в цілому, яка має доказове значення у кримінальному провадженні та пропонує використання комп'ютерної мережі в процесі доказування [254, с. 21].

В. В. Мурадов (2013) розмежовує електронні речові докази і електронні докази-документи [176].

Проте у науковому дискурсі існує і протилежна позиція, що аргументує необхідність виділення електронних (цифрових) доказів як самостійного процесуального джерела. Так, на думку Д. М. Цехана (2013), цифрова інформація з урахуванням унікальних характеристик не може бути віднесена до жодної класифікаційної групи, тому слід запровадити категорію «цифровий доказ» [283, с. 259].

Ю. Ю. Орлов та С. С. Чернявський (2017) пропонують позначати електронні документи спеціальним терміном «електронне відображення» й вважати самостійним джерелом доказів у кримінальному провадженні та окремим видом доказів. З огляду на це варто доповнити КПК України статтею 100-1 «Електронні відображення» [181, с. 116-117].

Д. О. Алексєєва-Процюк та О. М. Брисковська (2018) вважають, що доцільно електронні докази як різновид доказів виокремити в окреме джерело доказів, і не розглядати їх як різновид документа, доводячи потребу введення в КПК України окремої статті чи низки статей, які б стосувались інституту електронних доказів [7, с. 252]. С. О. Ковальчук (2018) зазначає, що на підставі норм КПК України, слідчої та судової практики електронні докази на сьогодні розглядаються як електронні

документи, а їх матеріальні носії – як речові докази. Проте, з урахуванням їх існування в електронній формі та механізму залучення у кримінальне провадження, електронні докази, за аналогією з їх закріпленням в адміністративному, господарському і цивільному процесах, доцільно визнати самостійним видом доказів у кримінальному процесі [139, с. 123]. Л. М. Перцова-Тодорова (2020) вказує, що слід вирізнити електронний доказ серед інших видів доказів і надати йому окремий статус шляхом внесення змін до КПК України, зокрема окремою нормою «електронні докази» з визначення змісту поняття, ознак та різновидів [189, с. 246-247]. Віднесення електронного документа до певного різновиду джерел доказів не може забезпечити його правильне використання у доказуванні, стверджує А. В. Гутник (Ратнова) (2021) [240, с. 41]. Науковиця пропонує доповнити ч. 2 ст. 84 КПК України п'ятим процесуальним джерелом доказів – електронний документ [240, с. 42], а також ст. 99-1 під назвою «Електронні документи» [240, с. 48]. Н. В. Глинська, Д. І. Клепка (2023) теж підтримують цю позицію [50, с. 59]. А.-М. Ю. Ангелюк (2023) вказує, що електронні докази повинні бути визнані окремим джерелом доказів, а також доводить необхідність визначення у нормах КПК України переліку можливих джерел отримання електронних доказів, які надалі стануть частиною кримінального провадження [8, с. 218].

Альтернативний підхід зводиться до трактування доказів електронної форми не як окремої категорії, а як способу фіксації вже наявних джерел доказової інформації.

В. М. Глібко (2016) вказує, що за способами фіксації документи поділяються на: письмові (тексти, цифрові записи, машинописні документи); фотодокументи; графічні документи (малюнки, схеми та ін.); кіно-відео документи; фотодокументи; електронні документи. Тобто вчений визначає електронні документи як один зі способів фіксації документів [51, с. 1-11]. Електронний спосіб фіксації це цілеспрямована діяльність суб'єктів збирання доказів, яка полягає у складанні протоколів процесуальних дій та додатків до них. Електронний спосіб фіксації (повністю або частково) може здійснюватися як щодо електронних документів, так і до інших джерел доказів – речових доказів, показань учасників кримінального

провадження. Спосіб фіксації визначає кінцевий вигляд доказу: повністю електронний (електронне процесуальне оформлення) чи змішаний (процесуальне оформлення на паперовому носії) [258, с. 120].

Попередньо автором (2019) підтримувалась позиція, що наявні у кримінальному процесі України джерела доказів та формат їх процесуального оформлення, рівень розвитку ІТ об'єктивно не дозволяють заявляти про виокремлення електронних доказів як окремого джерела, однак можемо говорити про їх електронну фіксацію. Вбачалося, що застосовуваний в сучасній правовій науці та практиці термін «електронні докази» повинен мати виключно теоретичне оформлення, а штучно створений інститут електронних доказів – не підміняти електронну форму їх фіксації [260, с. 188].

Викладені тези сьогодні не можуть бути підтвердженими й застосовуваними сучасною правовою наукою. Наш більш ніж десятирічний досвід безпосередньої практичної роботи представником сторони обвинувачення з доказами в електронній формі, останні шість років теоретичного дослідження у цій сфері, а також результати проведених нами в Тренінговому центрі прокурорів України, а також у співпраці з проектами Ради Європи понад 40 тренінгів для прокурорів, суддів та представників органів досудового розслідування, дало нам можливість усвідомити багатогранність досліджуваного правового явища та його надзвичайну складність. Тож спробуємо розглянути досліджувану проблематику концептуально й комплексно.

В академічному дискурсі окреме місце посідає підхід, за яким розглядають цифрову інформацію як теоретичну конструкцію, що відображає форму існування інформації.

О. П. Метелев (2018) вважає основними причинами виділення цифрової інформації, зафіксованої на машинних носіях, як самостійного і специфічного джерела відомостей, що не входять ні до складу речових доказів, ні до складу документів, її особливу нематеріальну природу, природно-технічні особливості її створення, обробки, зберігання, передачі в часі й просторі, а також кримінально-процесуальні процедури та техніко-криміналістичні прийоми її пошуку та

вилучення, доступу до неї, дослідження і перетворення її в форму, яку сприйматиме людина. У такому разі необхідно оцінювати власне інформацію, а не матеріальний об'єкт, на якому вона зафіксована. Крім того, для набуття доказового значення цифрова інформація повинна бути спеціальним чином перетворена із системи дискретних сигналів різної фізичної природи в форму, яку може сприймати людина. Так, наприклад, зміст документальної інформації, яка міститься в електронних документах чи файлах баз даних, звукових файлів чи фонограм, може бути перетворений у візуальну інформацію або шляхом її роздрукування на паперовий носій, або шляхом її виведення на екран монітора [170, с. 102-103].

Окремі науковці пропонують інституційну реконфігурацію КПК України, яка передбачала б не лише введення окремого джерела доказів, але й повне оновлення підходів до оцінки цифрової інформації, зокрема запровадження критеріїв автентичності, цілісності, достовірності, процедур збереження та верифікації.

Отже, панівним серед науковців та практиків є положення, що шляхом розширення переліку процесуальних джерел доказів, визначених ст. 84 КПК України, можна забезпечити належне процесуальне оформлення доказів в електронній формі. Водночас така концепція, попри її теоретичну і практичну значущість, виявляється недостатньою для комплексного розв'язання проблем, що породжуються розвитком ІТ, використанням криптовалют, даних з відкритих джерел здобутих за результатами Open Source Intelligence (далі – OSINT), мобільних пристроїв, хмарних сервісів, блокчейн-реєстрів тощо.

Потреба у правовому визначенні статусу, режиму збирання, фіксації, аналізу та використання відповідної інформації не зводиться лише до категоріального впорядкування джерел доказів. Ідеться про формування єдиного міждисциплінарного підходу, який передбачав би системне оновлення кримінального процесуального законодавства України та створення спеціалізованих підзаконних НПА, що регламентують технічні аспекти роботи з цифровою інформацією та технічними пристроями. Крім того, актуальним є впровадження стандартизованих операційних процедур (далі – СОП) для органів

досудового розслідування, а також підготовка й постійне навчання слідчих, прокурорів, суддів щодо особливостей роботи з доказами електронної форми.

З урахуванням вищевикладеного, слід визнати, що хоча теоретичні напрацювання вітчизняної науки в цьому напрямі є цінними й заслуговують на високу оцінку, подальший розвиток інструментів процесуального регулювання має виходити за межі формального доповнення переліку джерел доказів. Необхідним є системне реформування законодавства, зорієнтоване на практичну ефективність, технічну адекватність і відповідність цифровій реальності.

Особливості техніко-інформаційної природи електронних об'єктів у кримінальному провадженні безпосередньо впливають на способи їх класифікації. У зв'язку з цим актуалізується систематизація підходів, запропонованих у сучасній кримінальній процесуальній літературі, з метою встановлення методологічних орієнтирів для класифікації доказів електронної форми. Науковці пропонують класифікаційні підходи, виходячи з різних підстав: юридичної сили, технічної форми, походження, доступності метаданих, характеру носія, форми фіксації інформації тощо. Ці підходи суттєво відрізняються не лише за змістом, але й за обраною методологією. Так, О. В. Шведова (2006) пропонує поділяти електронні документи на дві групи: 1) документи, які можуть бути перенесені на фізичний носій інформації та не мають юридичної сили; 2) документи, які мають юридичну силу без їх перенесення на фізичний носій і мають електронний підпис, що дає можливість ідентифікувати особу, яка створила документ [290].

С. Й. Гонгало (2013) стадіями виготовлення електронні документи поділяє на оригінали, дублікати, копії та витяги [54, с. 34], а з точки зору використання електронного документа як доказу – юридичні та технічні. Юридичні документи містять передбачені законом реквізити, складаються уповноваженою на те особою та мають юридичну силу. До технічних документів слід відносити документи, які не мають юридичної сили [56].

Р. І. Благута та А. В. Мовчан (2020) видами цифрових (електронних) доказів називають таке: локальні сліди; мережні сліди; електронна інформація [24, с. 113-114].

Деякі автори (2019) наводять таку класифікацію електронних носіїв: інформації магнітно-оптичні; напівпровідникові; магнітні. Оптичні – CD-ROM; DVD-ROM. Магнітно-оптичні – (MO). Напівпровідникові – твердотілий на основі Flash пам'яті (SSD); USB Flash Drive (флешка). Магнітні – жорсткі диски, дискети, стримери [32, с. 15].

До так званих технічних електронних документів, що не мають юридичної сили, А. В. Гутник (Ратнова) (2021) відносить: фотографії та зображення, відео- та аудіозаписи, вебсайти, облікові записи у соціальній мережі, дані геолокації, голосові, мультимедійні та інші повідомлення, історія вхідних та вихідних викликів, записи, що містяться у нотатках, диктофоні, чернетках й навіть відмітки у календарях, у разі якщо вони можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. До юридичних електронних документів належать договори, різного виду звіти, акти, свідоцтва, витяги, протоколи, електронні платіжки та інші документи, які створюються в порядку електронного документообігу між державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності [240, с. 58]. Науковиця пропонує класифікувати електронні документи з таких підстав: за стадіями виготовлення; за комбінацією метаданих; залежно від доступу до метаданих електронного документа; за ступенем захисту; за джерелом походження; за їх місцем розташування; за формою [240, с. 184].

Усі перелічені підходи засвідчують значний ступінь гетерогенності у розумінні структури та природи доказів електронної форми а також акцентують на потребі доктринального уточнення класифікаційних критеріїв. На цьому етапі розвитку науки жодна з класифікацій не отримала загальноновизнаного статусу, що зумовлює потребу в уніфікації підходів та подальшому осмисленні цієї інституційної моделі. У цьому контексті варто вказати, що спроба розробити класифікацію, котра повністю охопила б докази електронної форми в кримінальному процесі, вбачається проблематичною з огляду на величезне коло об'єктів, що на практиці можуть набувати електронної форми та бути потенційно використаними у доказуванні.

Фінальним аспектом постає проблема термінологічної невизначеності, яка супроводжує все вищенаведене. Дефініційний плюралізм, що властивий сучасній доктрині, відображає відсутність усталеного підходу до правової категоризації доказів електронної форми. Це потребує критичного осмислення відповідної термінології.

Аналіз наукової літератури свідчить про відсутність уніфікованої термінології для позначення доказів електронної форми в кримінальному процесі України. У вітчизняному дискурсі паралельно функціонують десятки дефініцій, що значною мірою схожі за змістом, але мають різні акценти залежно від наукового підходу, технічної площини дослідження або спеціалізації автора.

Найчастішим у науковій літературі є термін «електронні докази». Його використовують у широкому значенні — як дані в електронній формі, що мають доказове значення у кримінальному провадженні. Однак цей термін не є усталеним і викликає численні заперечення щодо точності відображення природи відповідного явища. Наприклад, О. І. Котляревський та Д. М. Киценко (1998) під електронними доказами розуміють сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах [150; 7, с. 251].

П. Д. Біленчук, А. П. Гель, Г. С. Семаков (2007) зазначають, що електронні докази – це сукупність інформації, яка зберігається в електронному вигляді на всіх типах електронних носіїв і в електронних засобах [21, с. 451], тобто формулюють його майже без змін. Інші дослідники електронними доказами називають фактичні дані, які зберігаються в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах та які після обробки спеціальними технічними засобами та стають доступними для сприйняття людиною [7, с. 250]; дані, які підтверджують факти, інформацію або концепцію у формі, придатній для обробки за допомогою комп'ютерних систем, у тому числі програми виконання комп'ютерною системою або інших дій [13, с. 125]; інформація, що зберігається в електронному вигляді на будь-яких типах електронних носіїв, в електронних пристроях чи електронних інформаційних системах та відповідає вимогам ст. 84

КПК України [74, с. 112]. Водночас варто зауважити, що останнє визначення сформульовано як теоретична категорія для окреслення не окремого нового джерела доказів, а явища як такого [260, с. 182].

Група науковців (2017) під електронними доказами розуміють докази у кримінальних провадженнях, які можна отримати в електронній формі [31, с. 4]. Аналогічне визначення пізніше дають М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін. (2020) [30, с. 5], О. О. Волков (2018) [35, с. 7].

І хоча сьогодні весь світ переходить саме на цифрову інформацію, у КПК України необхідно використовувати більш універсальний термін – електронні докази, під якими розуміються фактичні дані, що зберігаються в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах і які після обробки спеціальними технічними засобами та ПЗ стають доступними для сприйняття людиною [7, с. 250].

О. В. Сіренко (2019) вважає, що електронні докази – це дані про обставини, що мають значення для кримінального провадження і існують у нематеріальному вигляді у межах технічного носія чи каналу зв'язку, та сприйняття й дослідження яких можливе за допомогою технічних засобів та ПЗ [248, с. 211]. С. І. Хом'яченко та Т. О. Часова (2020) стверджують, що електронний доказ – це інформація (відомості), що має електронну (цифрову) форму про обставини, які підлягають обов'язковому доказуванню у кримінальному провадженні [281, с. 178]. О.Г. Козицька (2020) зазначає, що електронний доказ є цифровим об'єктом, який був засобом чи знаряддям вчинення кримінального правопорушення, зберіг електронно-цифрові сліди кримінального правопорушення, був предметом або об'єктом вчинення кримінального правопорушення або містить інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [140, с. 420].

А. Б. Антонюк та В. А. Русецька (2020) доводять необхідність визначати в законодавстві поняття «електронний доказ» як дані, що підтверджують факти, інформацію або концепцію в формі, пристосованої для обробки за допомогою комп'ютерної системи, в тому числі програми виконання комп'ютерною системою

тих чи інших дій [10, с. 85]. Н. М. Ахтирська (2022) для цілей власного дослідження використовує поняття, наведене в Посібнику з питань електронних доказів для співробітників правоохоронних органів, прокурорів та суддів (2020) [71, с. 12], у якому електронними доказами вважається будь-яка інформація, що генерується, зберігається або передається в цифровій формі, і яка згодом може знадобитися для підтвердження або спростування факту, оскаржуваного в межах провадження. Попри те, що в різних юрисдикціях норми можуть відрізнятися, загалом під час оцінювання електронних доказів для судового розгляду слід враховувати такі критерії як автентичність, повнота, надійність, переконливість, пропорційність [12, с. 189]. Л. В. Мілімко, Я. В. Жидовцев (2025) під поняттям «електронний доказ в кримінальному провадженні» розуміють інформацію про факти та обставини кримінального провадження, що зафіксована в електронній формі та є відмінною від доказів в електронному вигляді й отримана в передбаченому кримінальним процесуальним законодавством порядку [172, с. 306].

Поряд із цим науковці визначають і використовують поняття «цифрові докази», що, на їх думку, краще відображає технічну сутність інформації, що обробляється цифровими засобами, представлена у вигляді бінарного коду і не має безперервної (аналогової) природи. Обґрунтовується перевага цього терміну як такого, що точніше фіксує кібернетичну природу збереження й обробки інформації в умовах комп'ютеризованого середовища. Так, Д. М. Цехан (2013) розглядає цифровий доказ як фактичні дані, представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія, що стають доступними для сприйняття людиною після обробки ЕОМ і на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження й підлягають доказуванню [283, с. 259]. О. П. Метелев (2018) визначає цифровий доказ як фактичні дані, отримані зі штучно створеного середовища і представлені у цифровій (дискретній) формі, зафіксовані на будь-якому типі електронних носіїв, стають доступними для сприйняття людиною за допомогою комп'ютерного обладнання, які вилучені, зафіксовані, досліджені та збережені відповідно до формалізованих процесуальних вимог,

встановлюють наявність чи відсутність фактів та обставин, що мають доказове значення для кримінального провадження [167, с. 82].

Г. Авдєєва, Е. Живуцька-Козловська (2023) зазначають, що термін «цифровий доказ» є більш точним і краще віддзеркалює сутність інформації в цифровій формі (у формі бінарного коду), а пристрої, засоби й машини, які створюють, передають, обробляють і зберігають цифрову інформацію, слід називати електронними. На думку вчених, цифровими доказами слід вважати фактичні дані, які представлені у вигляді бінарного (двійкового) коду та містять інформацію, що має значення для об'єктивного вирішення справи [4, с. 141].

Зустрічаються також використання деяких оригінальних термінів для позначення доказів в електронній формі. Наприклад, деякі вчені відкидають поняття «електронний документ» і пропонують інші визначення. Так, наприклад, В. В. Лисенко (2007) зауважив, що дослідники вживають «машинний документ», «документ, підготовлений з використанням електронно-обчислювальних машин», «комп'ютерна інформація» тощо, але сам пропонує термін «інформація, що міститься в електронному вигляді на будь-яких носіях» [160, с. 64]. І. О. Крицька (2016) зазначає, що комп'ютерну інформацію слід розглядати як частину всієї сукупності цифрової інформації. Але виходячи із положень ч. 1 та ч. 2 ст. 84 КПК України, більш доцільним видається використання категорії «цифрові джерела доказової інформації». Ця категорія об'єднує програми (ПЗ), файли баз даних, аудіо-, відеозаписи тощо, джерелом яких, а отже, і формою існування, виступають засоби цифрової техніки – машинні носії, до яких належать оперативні запам'ятовувальні пристрої, постійні запам'ятовувальні пристрої, накопичувачі на жорстких магнітних дисках (вінчестери, дискети), переносні машинні носії (оптичні носії, флешкарта), NAS-системи тощо [157, с. 302]. Також І. О. Крицька та деякі інші автори [7, с. 250] використовують термін «цифрова інформація» [157, с. 301]. Крім нього, в літературі зустрічаємо й такі як «кіберінформація» [13, с. 123], «цифрове алібі» [65, с. 31; 272, с. 1]; «електронні відображення» [181, с. 116–117], «електронний формат документа» [159, с. 161–162].

О. А. Самойленко (2020) ототожнює поняття «інформація в електронній формі», «електронні дані», «електронний документ». Вона вважає, що такий доказ не може існувати без носія інформації – джерела електронних даних як доказів, якими є різноманітні носії інформації (моноблоки, мобільні телефони, планшетні комп'ютери, цифрові камери, роутери, маршрутизатори, комп'ютерні мережі, глобальна мережа Інтернет, що містить звуко- та відеозаписи тощо;) невидимі «неозброєним оком» і для їх сприймання та дослідження використовують спеціальні програми та технічні засоби; також вони можуть пошкодитись, знищитись чи змінитись під час користування пристроєм, або під впливом різних чинників [243].

Додаткову складність становить термін «електронний документ», який сам по собі не є синонімом електронного доказу, але в окремих джерелах виступає як самостійна категорія або навіть виокремлюється як нове процесуальне джерело доказів. Так, А. В. Гутник (Ратнова) (2021) дає авторське визначення «електронних документів», під яким розуміються відомості в електронній формі, що можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [240, с. 184]. А. В. Коваленко (2022) вважає доцільним до закріплення в чинному кримінальному процесуальному законодавстві легальних визначень досліджуваних понять використовувати термін «електронні (цифрові) сліди (докази)». Вчений пропонує визначити електронні (цифрові) сліди кримінального правопорушення як комп'ютерні дані, що утворилися або зазнали змін у запам'ятовувальних пристроях електронно-обчислювальної техніки внаслідок дій користувачів, пов'язаних із вчиненням кримінального правопорушення [136, с. 233].

Варто також зауважити на окремі терміни, що мають вузькоспеціалізований або прикладний характер, що застосовуються для маркування конкретних категорій об'єктів. Їх наявність свідчить про динамічну еволюцію доказового інструментарію, однак ускладнює уніфікацію понятійного апарату.

Таким чином, концептуальний плюралізм у формуванні термінології свідчить як про трансдисциплінарну природу цифрової інформації, так і про брак

теоретичного консенсусу щодо її правового статусу. Аналіз наукових підходів до питання електронних (цифрових) доказів у кримінальному процесі України засвідчив глибоку структурну фрагментацію на рівні дефініцій, класифікацій та пропозицій щодо інтеграції цього явища у КПК України.

Множинність наукових досліджень є симптомом незавершеності теоретичного опрацювання проблематики. Попри наявність детальних пропозицій, жоден з існуючих підходів не отримав одностайної підтримки у процесуальній доктрині. Тож відсутність сталої нормативної конструкції унеможливорює ефективне розв'язання процесуальних питань, пов'язаних із фіксацією, зберіганням і верифікацією цифрової інформації в межах кримінального провадження. Розроблення цього напрямку має здійснюватися на основі міждисциплінарної методології, а змістовним орієнтиром має стати пошук не лише поняттєвої точності, а й процесуальної ефективності, органічної інтеграції доказів електронної форми в кримінальне процесуальне законодавство України з урахуванням особливостей функціонування правової системи в умовах цифрової трансформації.

Щоб сформулювати адекватну відповідь існуючим викликам, необхідно з'ясувати підстави формування інституту електронних (цифрових) доказів в науці кримінального процесу України, якими вважаємо таке:

1) впровадження останніх Законом України «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» від 03.10.2017 № 2147-VIII;

2) відсутність єдиного розуміння правниками процесуальної та технічної природи доказів електронної форми;

3) ратифікація Конвенції про кіберзлочинність, що потребувала імплементації і наукового дослідження [148, с. 1]. Щоправда, вказана Конвенція оперує категорією «докази в електронній формі»;

4) упровадження іноземними юрисдикціями інститутів електронних доказів у національне кримінальне процесуальне законодавство. Яскравим прикладом є Кримінальний процесуальний закон Латвії, що містить ст. 136 «Електронні

докази», та де вказується, що доказами в кримінальному процесі можуть бути відомості про факти у формі електронної інформації, обробленої, збереженої або переданої пристроями або системами автоматизованої обробки даних [439, с. 1]. Використання терміна «electronic evidence» у документах, рекомендаціях та посібниках Ради Європи; використання іноземними вченими категорій «electronic evidence» [71; 386; 388; 505 ; 454] та «digital evidence» [347], «computer evidence» [350] та «computer-based electronic evidence» [532];

5) технологічний тиск, що спричинив стрімке зростання в кримінальних провадженнях кількості доказів електронної форми та необхідність їх однотипного іменування під час дослідження й формулювання відповідних дефініцій.

Таким чином, передумови формування інституту електронних (цифрових) доказів у кримінальному процесі України полягають не лише у зовнішньому технологічному тиску, що спричинило стрімке зростання в кримінальних провадженнях кількості доказів електронної форми, а й у внутрішній потребі доктрини запропонувати відповідне правове регулювання, а також віднайти оптимальний баланс між стабільністю правозастосування та динамікою цифрових трансформацій. Врешті, відповідний правовий феномен необхідно було якось називати, що й спричинило термінологічну міграцію та сформоване практикою творення нових дефініцій.

У сучасних умовах функціонування кримінального судочинства всі об'єкти, які потенційно можуть бути віднесені до категорії електронних або цифрових доказів, у межах чинної чотирикомпонентної моделі джерел доказів, передбаченої ст. 84 КПК України, переважно залишаються формально розподіленими між такими процесуальними джерелами доказів, як документи та речові докази. При цьому низка цифрових об'єктів, особливо дані з відкритих джерел (наприклад, результати OSINT), фактично перебуває у правовому вакуумі — через брак усталеної позиції щодо можливості їх інтеграції у традиційну доказову систему, зокрема з урахуванням дискусій щодо матеріальної природи документа як джерела доказу в кримінальному процесі.

Ідея запровадження нового процесуального джерела доказів під назвою «електронні докази» або ж «цифрові докази», що реалізована у 2017 році в ЦПК України, ГПК України та КАС України, так і не була імплементована в КПК України. На нашу думку, цей факт обумовлений об'єктивними чинниками, насамперед неготовністю системи кримінальної юстиції до такого переходу. Запровадження такого нового джерела доказів вбачається проблематичним, чи навіть і неможливим без:

а) чіткого бачення сфери його охоплення – тобто визначення потенційного переліку об'єктів, що можуть кваліфікуватися як цифрові або електронні докази;

б) виразного розмежування цього нового джерела з такими, як документи та речові докази – на рівні змісту, форми, джерела походження та способу дослідження, взаємоузгодження зі всіма джерелами доказів;

в) адекватного уявлення про перехідний період – включаючи правила допустимості, належності та достовірності доказів, що були зібрані до моменту змін, а також нормативного механізму збереження їх процесуального статусу.

Особливої актуальності ця проблема набуває в контексті потенційного встановлення посилених технічних вимог до нової категорії доказів, зокрема обов'язкового підтвердження їхньої цілісності через гешування чи інші криптографічні засоби. У таких умовах сторона захисту, апелюючи до принципу *favor defensionis* [165], матиме підстави клопотати про застосування нових, сприятливіших норм доказування щодо доказів, зібраних до набрання чинності такими «посиленими» нормами КПК України. Це, своєю чергою, здатне створити нормативну колізію, що потенційно паралізує дієздатність механізмів кримінального переслідування, породжуючи юридичну невизначеність і масові оскарження вже зібраних доказів.

На нашу думку, саме усвідомлення масштабності та системного характеру зазначених ризиків і зумовило відмову законодавця від запровадження цього нового процесуального джерела доказів у КПК України. Такий стриманий підхід, попри критику, на сьогодні залишається виправданим задля забезпечення

стабільності кримінального процесу та недопущення правового колапсу в умовах високої динаміки цифрової трансформації.

Упродовж останніх десятиліть у вітчизняній кримінальній процесуальній науці сформувалося стійке уявлення про те, що актуалізовані цифровою трансформацією виклики кримінального судочинства можуть бути нейтралізовані шляхом доповнення переліку джерел доказів, визначених ст. 84 КПК України, елементами, які відображають новітні цифрові реалії. На перший погляд, такий підхід видається логічним, адже дає змогу формалізувати визнання досліджуваної форми доказів у межах чинної процесуальної конструкції. Проте, як показує аналіз практики застосування норм КПК України, а також міждисциплінарне осмислення змісту цифрових даних та носіїв інформації, така модель є лише частковим вирішенням значно глибших і багатогранніших проблем.

Потреба у нормативному врегулюванні особливостей роботи з цифровими даними, що охоплює питання цифрових носіїв, результатів OSINT, криптовалютних транзакцій, хмарних інфраструктур та іншого, не може бути зведена до простої легалізації нових джерел доказів. Сучасні цифрові реалії доволі часто не вкладаються у класичну модель доказів, побудовану на матеріальних носіях, а отже потребують вироблення нових методологічних та процесуальних підходів. Це, своєю чергою, передбачає потребу в створенні СОП для правоохоронців, уніфікації процесів виявлення, вилучення, фіксації та зберігання цифрової інформації, а також запровадження системного навчання відповідних суб'єктів кримінального провадження.

Попри серйозну теоретичну базу, що склалась завдяки зусиллям провідних учених, одне лише введення нового процесуального джерела доказу не усуває ключових викликів, а відтак необхідне усвідомлення того, що докази електронної форми мають бути переосмислені як самостійна системна реальність, що потребує адекватного, комплексного, технологічно орієнтованого нормативного супроводу.

1.4. Процесуальна та технічна природа доказів електронної форми у кримінальному процесі України

При дослідженні процесуальної природи доказів електронної форми насамперед необхідно загалом розглянути чинники та умови формування доказів під час кримінального провадження.

Залежно від форми вираження у фізичному середовищі інформація, або ж фактичні дані, можуть мати дві форми: 1) матеріальна – мають фізичне вираження відповідно до своєї матеріальної природи, їх існування в просторі не залежить від процесуального оформлення під час кримінального провадження таких фактичних даних. До цієї категорії належать різноманітні фізичні сліди, носії інформації (в тому числі енергонезалежні електронні носії інформації), речі та предмети фізичного світу. Матеріальні об'єкти можуть існувати тривалий час без процесуального оформлення та бути виявленими через багато років; 2) нематеріальна – фактичні дані не мають фізичного вираження, а надання фізичної (матеріальної) форми вимагає активних дій суб'єктами кримінального провадження – їх фіксації під час кримінального провадження (переважно досудового розслідування). Нематеріальні об'єкти мають властивість змінюватись, деградувати або ж зникати без процесуального оформлення. До цієї нематеріальної категорії належать відомості про події, дії, явища та стани (характеристики об'єкта в певний момент часу), що відбуваються в динаміці (сюди варто також віднести кіберпростір та всі види енергозалежної пам'яті комп'ютерних систем) та які можуть: бути сприйнятими людиною та зафіксуватися в її пам'яті; фіксуватися за допомогою фотографування, аудіозапису, відеозапису чи інших форм електронної фіксації інформації; при відсутності спостерігача або технічної фіксації зазнати змін з плином часу та не залишити будь-яких видимих слідів.

З огляду на це, інформація нематеріальної категорії може отримати два вираження, серед яких: а) ментальна, тобто пам'ять (свідомість) людини, що зберігає інформацію про певні події чи явища. З плином часу події злочину, зафіксовані у свідомості людини, мають властивість деградувати та змінюватись,

тому оперативність їх фіксації корелюється з точністю; б) цифрова – бітовий рядок даних, що представлений зазвичай послідовністю одиниць та нулів. Цифрова інформація має нематеріальну природу, віддільна від носія інформації й існує у формі бітової послідовності. Вона реалізується через електронний носій інформації, що виконує функцію контейнера, а її сприйняття можливе лише за допомогою технічних засобів, що забезпечують декодування та візуалізацію змісту даних.

З метою збереження фактичних даних про події, дії, явища та стани під час досудового розслідування здійснюється фіксація нематеріальної інформації у ході проведення слідчих (розшукових) дій та НСРД у встановленому законом порядку. Таким чином, джерело інформації перетворюється на доказ у певному кримінальному провадженні шляхом процесуального оформлення, здійсненого у визначеному КПК України порядку [260, с. 185]. Наприклад, обставини події злочину, зафіксовані у пам'яті людини, встановлюються та фіксуються під час проведення допиту; предмети вилучаються під час проведення обшуку; цифрова інформація фіксується під час проведення огляду; ознаки предметів або процесів встановлюються при проведенні експертного дослідження. Тобто під час досудового розслідування доказ долучається до матеріалів кримінального провадження шляхом його процесуального оформлення – фіксації відповідно до вимог КПК України, та в окремих випадках набуває матеріальної форми існування [107, с. 63-64].

Процесуальне оформлення – спосіб закріплення доказів з метою їх збереження в порядку, визначеному КПК України, для наступного дослідження та використання під час кримінального провадження. Процесуальне оформлення передбачає фіксацію певної події, факту чи предмета та посвідчення отриманих матеріалів, що може бути здійснено на паперовому носії або електронному (фіксація на відео, аудіо, фото, у формі електронного протоколу тощо) [74, с. 113].

Відповідно до ст. 103 КПК України, процесуальні дії під час кримінального провадження можуть фіксуватися: 1) у протоколі (згідно з вимогами ст. 104 КПК України); 2) на носії інформації, на якому за допомогою технічних засобів

зафіксовані процесуальні дії (які відповідно до п. 3 ч. 2 ст. 99 КПК України віднесено до документів); 3) у журналі судового засідання (згідно з вимогами ст. 108 КПК України) [107, с. 64].

Під час досудового розслідування кримінального провадження докази (незалежно від своєї первинної форми – матеріальної чи нематеріальної) мають бути письмово (за допомогою засобів письма) процесуально оформлені, вимога щодо чого опосередковано визначена в нормах ст. ст. 103-104 КПК України. Проте жодна з норм не містить вимоги щодо фізичної форми існування такого протоколу, його паперового формату. При цьому норми Закону України «Про електронні документи та електронний документообіг» встановлюють вичерпні вимоги до форми електронного документа, що застосовні також відносно кримінального провадження [107, с. 64]. Тож варто визнати потенційну можливість існування доказів у електронній формі на сучасному етапі реалізації кримінального провадження щодо кожного з процесуальних джерел доказів, визначених у ст. 84 КПК України: показання, речові докази, документи, висновки експертів.

В історичній ретроспективі матеріалізація доказу пов'язана з необхідністю його фіксації, класичний приклад – фіксація показань особи (потерпілий, свідок, підозрюваний тощо) за допомогою їх запису на папері й долучення такого матеріального письмового доказу до матеріалів кримінального провадження. Цікаво, що зараз така фіксація показань особи може бути здійснена також за допомогою відеозапису. При цьому носій інформації з відповідним відеозаписом долучається як додаток до матеріального паперового протоколу допиту. Тобто матеріальна форма існування, як властивість такого виду доказу як показання, так чи інакше зберігається [107, с. 65]. Це застосовне також щодо фіксації слідчих (розшукових) дій за допомогою технічних засобів. Вказане передбачає, що запис, здійснений за допомогою звуко- та відеозаписувальних технічних засобів під час проведення слідчим, прокурором обшуку, є невіддільним додатком до протоколу (ч. 2 ст. 104 КПК України).

Важливо зауважити, що на сьогодні кримінальне процесуальне законодавство України не містить обмежень щодо виготовлення під час

кримінального провадження процесуальних документів у електронній формі, а також вимог щодо їх обов'язкового існування у формі традиційних томів паперових документів. Ба більше, тепер вже існує нормативна та технічна основа для фіксації кримінального провадження в електронній формі, адже КПК України не забороняє виготовлення та використання електронних процесуальних документів, а у всіх дізнавачів, слідчих, детективів та прокурорів є електронні підписи, що обумовлено необхідністю роботи з ЄРДР. Однак загалом практика правозастосування на сьогодні визначає матеріальну форму існування обов'язковою властивістю доказу в кримінальному процесі України, незалежно від форми первинної інформації, що є джерелом відповідного доказу [107, с. 67].

Необхідно чітко розмежувати фактичні дані, що мають нематеріальну цифрову (бітову) природу, та фіксацію доказів у електронній формі за допомогою технічних засобів. На остаточний формат доказу в однаковій мірі впливають як характер джерела інформації, так і процесуальне оформлення [260, с. 185] за умови адекватного вибору формату останнього.

У контексті зазначеного варто наголосити на необхідності адекватного вибору способу фіксації відомостей під час кримінального провадження, що має обумовлюватися природою інформації, що підлягає фіксації, а також обставинам, за яких ця фіксація здійснюється. Зокрема, для фіксації показань умовно релевантним є фіксація у формі письмового протоколу, однак в умовах воєнного стану доцільно застосовувати відеозапис. Указане в перспективі уможливить використання також показань як доказів в суді у порядку ч. 11 ст. 615 КПК України. Щодо фіксації обшуку житла чи іншого володіння особи на підставі ухвали слідчого судді ч. 10 ст. 236 КПК України визначає обов'язкове застосування аудіо- та відеозапису. Щодо огляду така імперативна вимога визначена в ч. 2 ст. 237 КПК України (як бланкетна) лише щодо огляду житла чи іншого володіння особи, що може спричинити неоднозначні ситуації. Зокрема, в абз. 2 ч. 2 ст. 237 КПК України вказується, що огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів,

фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі). Разом з тим імперативної вимоги щодо фіксації змісту комп'ютерних даних у цифровій формі законодавцем не вказано. Наприклад, огляд вебсторінки можна реалізувати шляхом письмового опису її змісту та фотографування екрана комп'ютера (практиці відомі такі випадки), що формально не суперечитиме вимогам КПК України. Однак для ефективної фіксації змісту вебсторінки необхідно окрім іншого також зберегти її HTML-версію, архівувати (наприклад, за допомогою Wayback Machine - інтернет-архіву, що зберігає копії веб-сторінок у визначений момент часу), виготовити скріншот тощо (відповідно до вимог Протоколу Берклі як усталеної міжнародної практики).

Відтак релевантність способу фіксації вимагає оцінки не лише формальної відповідності дій суб'єктів кримінального провадження вимогам КПК України, а передусім – комплексу ознак, що визначають можливість підтвердження автентичності та цілісності зафіксованої інформації при її використанні як доказу в кримінальному провадженні. Йдеться про необхідність забезпечення: технічної адекватності обраного способу фіксації до природи цифрового об'єкта (зокрема, його мінливості, формату, способу існування у віртуальному середовищі); відтворюваності зафіксованих даних з метою їх подальшої перевірки, дослідження та представлення в суді; гарантій достовірності, що передбачає можливість підтвердження цілісності інформації з використанням метаданих, геш-значень, електронних підписів або архівування; процесуальної справедливості, яка виявляється у дотриманні принципу мінімального втручання та недопущенні спотворення або втрати значущої інформації через вибір неадекватного способу фіксації. У такий спосіб технічна та юридична релевантність фіксації даних повинні розглядатися як взаємозалежні умови допустимості доказу електронної форми.

У цьому аспекті також доцільно диференціювати категорії вимог до суб'єктів кримінального провадження в частині фіксації під час кримінального провадження відомостей, які стануть доказами електронної форми:

а) вимоги коректного поводження з цифровими об'єктами та явищами, що передбачає вимоги до суб'єкта кримінального провадження щодо коректного та технічно грамотного поводження з: комп'ютерними системами та комп'ютерними пристроями з метою забезпечення цілісності та незмінності інформації, що на них зберігається; статичними об'єктами, що мають цифрову природу (електронні носії інформації, документи, електронні документи в розумінні Закону України «Про електронні документи та електронний документообіг» тощо) для забезпечення їх збереженості та належної правової оцінки під час кримінального провадження; відомостями, що мають цифрову форму та існують в нематеріальному середовищі (кіберпростір або RAM) для забезпечення їх належної фіксації, підтвердження автентичності (chain of custody) та забезпечення цілісності;

б) вимоги до фіксації відомостей під час кримінального провадження в електронній формі, що передбачає вимоги до суб'єкта кримінального провадження щодо коректного та технічно грамотного: виготовлення протоколу або іншого процесуального документа в електронній формі; виготовлення додатків до протоколів та їх зберігання на електронних носіях інформації.

З огляду на наведену класифікацію, можемо виокремити відповідні п'ять напрямів, що потребують аналізу при дослідженні нами кожного з процесуальних джерел доказів як таких, що потенційно можуть мати електронну форму. Подальший аналіз джерел доказів у контексті їх потенційного відображення в електронній формі ілюструє цікаві тенденції, що вимагають системного аналізу процесуальних джерел доказів у контексті їх існування в електронній формі.

Згідно зі ст. 84 КПК України існує чотири процесуальні джерела доказів: показання, речові докази, документи, висновки експертів [155, с. 1]. Зараз перед науковцями та практиками кримінального процесу постає питання, до якого з процесуальних джерел доказів, визначених ст. 84 КПК України, належать докази електронної форми.

Щодо такого процесуального джерела доказів як документи нам пощастило мати цінний науковий фундамент, що його складають праці вітчизняних процесуалістів, зокрема А. В. Гутник (Ратнової) (2021), яка досліджує кримінальні

процесуальні та криміналістичні основи використання електронних документів у доказуванні [156; 240], та А. В. Скрипника (2021), який вивчає використання інформації з електронних носіїв у кримінальному процесуальному доказуванні [249]. Тому не вважаємо доцільним знову звертатися до проблем, що вже порушувалися нашими попередниками, позаяк кардинальних змін у КПК України у досліджуваному контексті не сталося. Згадані роботи є досить ґрунтовними й цікавими, тож ми приділимо увагу іншим аспектам досліджуваної проблематики.

У частині 1 ст. 99 КПК України документ визначається як «спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження». Згідно з ч. 2 ст. 99 КПК України до документів, за умови наявності в них відомостей, передбачених ч. 1 ст. 99 КПК України, можуть належати: 1) матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані); 2) матеріали, отримані внаслідок здійснення під час кримінального провадження заходів, передбачених чинними міжнародними договорами, згоду на обов'язковість яких надано Верховною Радою України (далі – ВР України); 3) складені в порядку, передбаченому КПК України, протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії; 4) висновки ревізій та акти перевірок; 5) довідки, висновки та інші документи спеціалістів.

Розглядаючи документ як процесуальне джерело доказів, варто сформулювати такі групи об'єктів, що можуть розглядатись як докази електронної форми: матеріали фотозйомки, звукозапису, відеозапису (п. 1 ч. 2 ст. 99 КПК України); носії інформації (п. 1 ч. 2 ст. 99 КПК України); комп'ютерні дані (п. 1 ч. 2 ст. 99 КПК України); носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії (п. 3 ч. 2 ст. 99 КПК України); всі інші категорії (що визначені в ч. 2 ст. 99 КПК України або підпадають під визначення, наведене в ч. 1 ст. 99 КПК України) у формі електронних документів у розумінні Закону України «Про електронні документи та електронний документообіг».

За результатами проведеного нами опитування¹ суб'єктів кримінального провадження встановлено, що у відповідь на питання «Які типи електронних доказів у вашій практиці збираються (отримуються) в кримінальних провадженнях?» респондентам пропонувалася можливість обрати кілька варіантів відповіді, за результатами чого встановлено, що: результати фіксування (відеозаписи, фотознімки, аудіозаписи, скановані документи тощо) присутні в практиці 89% опитаних; електронне листування (через месенджери, електронну пошту, внутрішні сервіси сервера (внутрішні месенджери продукту для комунікації з операторами, іншими клієнтами тощо)) – 67%; електронні документи (юридичні документи з використанням електронних підписів, електронних сертифікатів походження або внутрішніх міток організації/сервісів) – 52%; програмні коди, програмні логи (запис діяльності, порушень програмного продукту), результати роботи програмного продукту (результати обробки інформації, запитів до сервісів тощо) – 16% (див. Додаток Б, Додаток В Рис. 3). Це вказує нам на певні види доказів, що є особливо актуальними для практичних працівників та потребують як належного правового регулювання, так і дослідження практики їх застосування, приділення уваги під час спеціалізованих тренінгів тощо [114, с. 80].

Аналіз статей 99, 103, 104 КПК України дає можливість провести розмежування електронних документів як джерел доказів та як способу фіксації такого доказу [240, с. 31]. По-перше, це час створення електронного документа. Електронний документ (листування, фотографії, відеозаписи тощо) можуть бути створені будь-ким та в будь-який час. Натомість електронний документ як спосіб

¹ В межах дисертаційного дослідження протягом березня-листопада 2024 року проведено опитування щодо практика роботи з доказами електронної форми в кримінальному процесі України. За результатами опитування, за допомогою онлайн форм та звичного паперового анкетування отримано відповіді 1356 респондентів. За наслідком опрацювання результатів опитування ряд анкет виключено. Отже, у цьому дослідженні проаналізовано релевантні відповіді 1301 респондента, серед яких: судді – 128; прокурори – 574; адвокати – 100; слідчі та детективи – 146; експерти та спеціалісти – 59; науковці – 120; оперативні працівники правоохоронних органів – 174 (з них: оперативні працівники кіберполіції – 21). Досвід роботи респондентів у галузі права є різноманітним та охоплює різні категорії: до 3 років – 4%; до 5 років – 2%; понад 5 років – 14%; понад 10 років – 33%; понад 15 років – 20%; понад 20 років – 16%; понад 25 років – 8%; понад 30 років – 3%. Ступінь залученості респондентів до роботи з доказами електронної форми (відповідь на питання «Як часто ваша робота пов'язана з доказами електронної форми?») також ілюструє охоплення всіх категорій, зокрема: дуже рідко (менше 10%) працюють з цією категорією доказів 14% опитаних; рідко (близько 30 %) – 15%; час від часу (близько 50%) – 28%; часто (близько 70%) – 26%; дуже часто (понад 90%) – 17%. В цілому ж, згідно з отриманими відповідями, середній рівень «присутності» досліджуваної категорії доказів становить 53,4%, що ілюструє їх високу розповсюдженість та є відверто величезним значенням з огляду на системні недоліки правового регулювання в цій сфері.

фіксації проводиться лише в межах досудового розслідування (після внесення відомостей до ЄРДР) та під час судових засідань у порядку, регламентованому КПК України [240, с. 31]. По-друге, здійснювати фіксацію доказу в електронній формі може лише уповноважений на те суб'єкт (слідчий, дізнавач, прокурор, секретар судового засідання), а створити електронний документ може будь-яка особа, або ж комп'ютерна система [240, с. 32]. По-третє, для формування електронного документа як доказу необхідно надати йому відповідну процесуальну форму. Така процедура здійснюється під час фіксації доказів. Електронний спосіб фіксацій є одним з різновидів фіксації доказів [240, с. 32].

А.С. Запотоцький (2009) вказує, що електронні документи з'являються у кримінальному провадженні, власне, у «готовому вигляді», а КПК України лише регламентує порядок їх збирання та дослідження, але не порядок складання. Форма, обов'язкові реквізити та порядок складання протоколів за результатами слідчих (розшукових) дій з метою дотримання достовірності доказів регламентовано у КПК України. Протоколи є завжди письмовими документами, які складені згідно з вимогами КПК України, тоді як електронні документи мають іншу форму [88, с. 9].

За способом фіксації відомостей документи пропонуємо класифікувати наступним чином: 1) паперові – письмові документи, що виготовлені шляхом написання або друку на папері; 2) документи електронної форми – документи, інформацію в яких зафіксовано у вигляді комп'ютерних даних; 3) електронні – документи, інформацію в яких зафіксовано у вигляді комп'ютерних даних та які мають обов'язкові реквізити електронного документа, що визначені в Законі України «Про електронні документи та електронний документообіг» [107, с. 65].

Чинний КПК України однаково визнає можливість використання під час кримінального провадження як паперового, так і електронного документа (ч. 3, ч. 4 ст. 99 КПК України). Отже, документ як доказ у кримінальному провадженні може мати як паперову, так і електронну форму.

Документи, що надані на запит або виявлені й вилучені під час слідчих (розшукових) дій та НСРД, можуть мати будь-яку з визначених форм. Документи,

створені за результатами проведення слідчих (розшукових) дій та НСРД, можуть мати як «класичну» паперову форму, так і електронну форму в розумінні електронного документа, визначеного законом. Комп'ютерні дані підлягають фіксації під час проведення слідчих (розшукових) дій та НСРД на певному носії інформації. У разі окремих НСРД поряд з «класичним» протоколом здійснюється також «розшифрування» розмов фігурантів такої НСРД. При цьому в усіх випадках складається письмовий протокол на паперових носіях, додатком до якого є носій інформації, на якому зафіксовано відповідні комп'ютерні дані, які зберігаються та передаються через режимно-секретні частини відповідних органів досудового розслідування та органів прокуратури [107, с. 66].

Згідно з ч. 3 ст. 99 КПК України оригіналом документа є сам документ, а оригіналом електронного документа – його відображення, якому надається таке ж значення, як документові [155, с. 1]. У контексті цієї статті варто розглядати електронний документ у розумінні Закону України «Про електронні документи та електронний документообіг».

Відповідно до ч. 4 ст. 99 КПК України дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невіддільних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа.

Отже, в КПК України з'явився альтернативний спосіб збирання інформації, що має електронну форму, – збирання доказів електронної форми шляхом копіювання інформації, для якого передбачено процесуальну форму, що можна представити як формулу: «копія інформації × (слідчий або прокурор + спеціаліст) = оригінал документа» [125, с. 337].

Конвенція про кіберзлочинність у п. «б» ст. 1 визначає термін «комп'ютерні дані» як «будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є

придатною для того, щоб спричинити виконання певної функції комп'ютерною системою» [148, с. 1]. Тобто правова природа даних, що їх потенційно можна отримати під час кримінального провадження за результатами OSINT, є доволі однозначною. Під час кримінального провадження OSINT здійснюється (переважно) під час проведення такої слідчої (розшукової) дії як огляд (ст. 237 КПК України), його результати фіксуються в протоколі, що складається за результатами проведення відповідної слідчої (розшукової) дії, а також може фіксуватися на носії інформації, на якому за допомогою технічних засобів зафіксовані процесуальні дії, тобто додатках до протоколу. З огляду на характер матеріалів, що отримуються за результатами OSINT, а також норми КПК України та ст. 1 Конвенції про кіберзлочинність, результати OSINT як джерело доказів у кримінальному провадженні, в контексті ст. 84 КПК України, є документом. Практика правозастосування та судова практика України дотримується аналогічної позиції, як такої, що відповідає чинному законодавству та елементарній логіці [116, с. 46-47]. Разом з тим варто зауважити, що в контексті розслідування воєнних злочинів результати OSINT становлять значну частину доказів, що вимагає належного обґрунтування не лише в національному контексті, а й у міжнародному. Проте тут простежуються певні проблемні питання, що вимагають належної уваги науковців. Зокрема, окремі закордонні колеги, з якими ми обговорювали питання використання доказів електронної форми в контексті воєнних злочинів та імена, яких не вказуватимемо з етичних міркувань, висловлювали свою думку про «нелегітимність» будь-яких результатів OSINT як доказів у кримінальних провадженнях. Це аргументувалося нормами ст. 99 КПК України, перекладеними англійською мовою. На погляд закордонних колег, теза ч. 1 ст. 99 КПК України «Документом є спеціально створений з метою збереження інформації матеріальний об'єкт» з акцентом на слово «матеріальний» (в англійському варіанті перекладу) унеможливорює використання всіх доказів, що не отримані під час проведення досудового розслідування у матеріальній (фізичній) формі. Також наводилися тези про вживання, на їх думку, різних термінів по тексту ст. 99 КПК України, що є звичним для нас, однак кардинально незрозумілим для іноземних правників.

Указана ситуація (всупереч певній її софістичності, на наш погляд) викликає занепокоєння і вимагає ефективного реагування наукової спільноти та здійснення подальшого дослідження наведеного проблемного питання з формуванням адекватної правової позиції, що може бути донесена до прихильників такої теорії «матеріальності документів у кримінальному процесі України» [116, с. 47-48].

Щодо речових доказів, дослідники слушно зауважують, що під час виявлення доказу в електронній формі у практиків часто постає питання, до якого з джерел доказів його відносити – речового доказу чи документа [240, с. 38; 177, с. 65]. В. В. Вапнярчук (2017) стверджує, що при розгляді документів як самостійного процесуального джерела доцільно звернути увагу на їх розмежування з іншими процесуальними джерелами. Наприклад, матеріальний об'єкт, який містить певну інформацію, є документом у разі коли він важливий лише своїм змістом. Якщо ж для провадження мають значення його інші якості (зовнішній вигляд, сліди, матеріал з якого виготовлений, місце чи час його знаходження тощо), тоді він набуває статусу речового доказу [27, с. 305].

Варто підтримати думку А. В. Коваленко (2018) про потребу перестати робити акцент на матеріальному носії інформації документа, адже у такому випадку документом вважається фізичний носій інформації, а не окремий файл, який міститься на ньому та має доказове значення. Крім того, на одному носії можуть міститись безліч файлів, а доказове значення у кримінальному провадженні мати лише один. Прив'язка документа до носія інформації, який існує в матеріальному вигляді, також спричиняє проблему вилучення інформації з інтернет-серверів, які, зазвичай, можуть знаходитись віддалено та доступ до яких отримати дуже складно, або неможливо [133, с. 239].

І. О. Крицька (2018) зазначає, що на практиці речовими доказами зазвичай визнаються саме матеріальні носії інформації (зокрема, системні блоки, флешкартка, оптичні диски тощо), а не електронні файли, операційне ПЗ, шкідливі програми, зафіксовані на них [158, с. 42]. Водночас для доказів електронної форми категорія «речові докази» може стати додатковим процесуальним статусом. Ним може бути наділений носій інформації, навіть якщо через призму норм КПК

України його можна теоретично зараховувати до такого процесуального джерела доказів, як документ, що відбувається за такою схемою.

Розроблена нами візуалізація (див. Додаток Г) відображає типовий алгоритм дій під час вилучення ЕНІ в межах обшуку, що має безпосереднє значення для правильного визначення його правового статусу в кримінальному процесі. Першим етапом є обшук, який згідно зі ст. 234 КПК України проводиться з метою виявлення та фіксації обставин вчинення кримінального правопорушення. На цьому носій інформації може бути виявлений як об'єкт, що потенційно містить докази. Другий етап – вилучення носія інформації, що реалізується в межах вимог ч. 7 ст. 236 КПК України. Саме на цій стадії виникає необхідність визначити напрям подальшої процесуальної роботи з вилученим об'єктом, який є тимчасово вилученим майном. Наступний можливий крок – визнання речовим доказом, який є вимушеним кроком у разі потреби накладення арешту на носій інформації як тимчасово вилучене майно, відповідно до вимог ч. 1 ст. 170 КПК України.

Таким чином, «статус» речового доказу впливає не з процесуальної природи доказу електронної форми, а є рішенням, спрямованим на збереження такого доказу в органу досудового розслідування (з метою дотримання норм КПК України щодо накладення арешту на тимчасово вилучене майно).

Варто наголосити, що доказ електронної форми, в частині цифрової інформації (комп'ютерних даних) є насамперед документом у розумінні ст. 84 КПК України. Постає потреба в чіткому порівнянні режиму роботи щодо документів і речових доказів (як процесуальних джерел доказів) у контексті деяких процесуальних норм.

Так, ст. 100 КПК України встановлює різні вимоги до збереження доказів. Відповідно до ч. 2 цієї статті речові докази, які отримані або вилучені слідчим, прокурором, оглядаються, фотографуються та докладно описуються в протоколі огляду. Зберігання речових доказів стороною обвинувачення здійснюється в порядку, визначеному Кабінетом Міністрів України. Це відповідає природі матеріального об'єкта, що безпосередньо пов'язаний із подією злочину. Натомість ч. 3 ст. 100 КПК України передбачає, що документ повинен зберігатися протягом

усього часу кримінального провадження. За клопотанням володільця документа слідчий, прокурор, суд можуть видати копії цього документа, за необхідності – його оригінал, долучивши замість них до кримінального провадження завірених копій. Таким чином, режим поводження з документом передбачає формалізований підхід до його збереження, у той час як речовий доказ розглядається як об'єкт візуального та матеріального контролю. У контексті ст. 236 КПК України фіксується важлива відмінність у повноваженнях слідчого, прокурора під час обшуку. Частина 7 цієї статті надає право слідчому або прокурору оглядати й вилучати документи, тобто здійснювати безпосереднє процесуальне втручання без додаткових умов. Натомість відсутність аналогічного стану справ у цій самій нормі створює обмеження для негайного огляду носіїв інформації, що є речовими доказами, адже відповідна частина статті дозволяє «проводити вимірювання, фотографування, звуко- чи відеозапис, складати плани й схеми, виготовляти графічні зображення ... окремих речей, виготовляти відбитки та зліпки, ... тимчасово вилучати речі, які мають значення для кримінального провадження». Конструкція ч. 7 ст. 236 КПК України фактично не надає слідчому, прокурору право оглядати речі під час проведення обшуку. Під час відкриття матеріалів кримінального провадження ст. 290 КПК України встановлює обов'язок сторони обвинувачення надати іншій стороні доступ до матеріалів досудового розслідування. Відповідно до ч. 3 цієї статті прокурор або слідчий за його дорученням зобов'язаний надати доступ та можливість скопіювати або відобразити відповідним чином «будь-які речові докази або їх частини», а також «документи або копії з них». Порівняльний аналіз цієї норми свідчить про однакову вимогу щодо відкритості інформації, проте реалізація доступу до документа може бути здійснена шляхом надання копії, тоді як до речового доказу – безпосередньо, що потребує зокрема організаційних заходів для забезпечення їх безпеки, унеможливлення пошкодження або знищення. У межах ст. 358 КПК України, що регулює питання дослідження документів під час судового розгляду, ч. 3 встановлює, що якщо долучений до матеріалів кримінального провадження або наданий суду особою, яка бере участь у кримінальному провадженні, для

ознайомлення документ викликає сумнів у його достовірності, учасники судового провадження мають право просити суд виключити його з-поміж доказів і вирішувати справу на підставі інших доказів або призначити відповідну експертизу цього документа. Вказане ілюструє процесуальну процедуру, що надає можливість встановити правдивість відповідного доказу. Отже, порівняння норм КПК України демонструє, що документи й речові докази у кримінальному провадженні регулюються різними процесуальними підходами, що впливають на способи їх використання, доступу, зберігання й оцінки. Узгодження цих режимів щодо доказів електронної форми та забезпечення цілісного підходу до їх нормативного оформлення є важливим елементом їх використання під час кримінального провадження [115, с. 85-92].

Доцільно розглянути розроблену нами схему (див. Додаток Д) як графічну візуалізацію складної структури співвідношення між фізичним об'єктом, що підлягає фактичному вилученню, та процесуальною ідентифікацією його окремих складових відповідно до положень КПК України.

Ця схема відображає диференціацію об'єкта вилучення на три структурні складники:

1. Цифрова інформація (комп'ютерні дані) — це змістовна складова, що становить безпосередній процесуальний інтерес для цілей доказування. У цифровій формі ця інформація репрезентується у вигляді бітових комбінацій (логічний код), що можуть бути ідентифіковані, зчитані, скопійовані або збережені. Ця інформація належатиме до такого процесуального джерела доказів як документ, відповідно до п. 1 ч. 2 ст. 99 КПК України як «комп'ютерні дані».

2. Носій інформації — фізичний пристрій або компонент комп'ютерної системи на якому зберігається відповідна цифрова інформація (наприклад, жорсткий диск, USB-накопичувач, плата мобільного телефону, компоненти пам'яті серверу тощо). Цей носій не є об'єктом безпосереднього процесуального інтересу і виступає в ролі об'єкта, що забезпечує існування цифрової інформації у фізичному світі (наприклад, у разі традиційного документа таким об'єктом є папір). З огляду на норми п. 1 ч. 2 ст. 99 КПК України цей носій інформації може бути віднесено до

такого процесуального джерела доказів як документ («носіє інформації»). Однак такий носій інформації також є майном особи, в якій він вилучається (адже має певну ціну і цінність, тоді як ціною аркуша паперу для класичних документів можна знехтувати), і його потенційний процесуальний статус як тимчасово вилученого майна вимагатиме подальшого накладення арешту.

3. Фізична оболонка пристрою або комп'ютерної системи (за наявності) – елемент, що представляє матеріальну структуру пристрою або комп'ютерної системи, що підлягає вилученню в межах кримінального провадження. У такому разі йдеться про майно особи та його потенційний процесуальний статус як тимчасово вилученого майна, що вимагатиме подальшого накладення арешту.

Запропонована схема розмежовує матеріальну та нематеріальну сутність об'єкта вилучення, що має ключове значення для визначення його складових через призму процесуальних джерел доказів як документа або речового доказу.

Ще одна розроблена нами схему (див. Додаток Е) концептуально окреслює дві моделі фіксації доказів електронної форми залежно від його походження та особливостей виявлення. Лівий блок схеми відображає ситуацію, коли цифрова інформація безпосередньо походить із кіберпростору (зокрема, інтернет-ресурсів, хмарних сервісів, публічних реєстрів, відкритих профілів тощо). Така інформація підлягає огляду і фіксації — із використанням стандартних або спеціалізованих програмних та технічних засобів, релевантних методів (виготовлення скріншотів, експорт HTML, архівування тощо). Результатом такої фіксації є цифрова інформація (комп'ютерні дані), що містить відомості, які мають значення для кримінального провадження, та належатиме до такого процесуального джерела доказів як документ, відповідно до п. 1 ч. 2 ст. 99 КПК України як «комп'ютерні дані». Правий блок схеми демонструє другу ситуацію – коли джерелом доказової інформації є комп'ютерна система, до якої був здійснений доступ у межах проведення слідчої (розшукової) дії, та під час цієї дії здійснено копіювання цифрової інформації шляхом створення образу носія інформації або ж криміналістичної (побітової) копії носія інформації (наприклад, у форматі .E01). Вказаний образ носія інформації належатиме до такого процесуального джерела

доказів як документ, відповідно до п. 1 ч. 2 ст. 99 КПК України як «комп'ютерні дані». Водночас комп'ютерні дані, що здобуті під час такої фіксації, повинні отримати фізичну форму, а відтак під час відповідних слідчих (розшукових) дій вони фіксуються на носіях інформації, що належатимуть до такого процесуального джерела доказів як документ, відповідно до п. 3 ч. 2 ст. 99 КПК України як «носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії». Такий носій інформації, на якому зафіксовані процесуальні дії, буде документом, адже не потребує врегулювання питання права власності на нього. Цей носій вже закуплений державою в особі органу досудового розслідування, так само як папір, на якому надруковано процесуальні документи. Коли ж носій інформації чи комп'ютерна система є власністю особи, необхідно встановити правовий режим щодо цього майна як власності, що наразі реалізується через такий захід забезпечення кримінального провадження, як арешт майна. Арешт майна можливий лише щодо речового доказу (див. Додаток Г), оскільки законодавець не передбачив такої легальної ситуації, за якої право власності на майно може бути обмежене з інших підстав. А у цих випадках саме така ситуація виникає і її потрібно врегулювати [115, с. 85-92].

Зокрема, необхідність утримання органом досудового розслідування цінного носія інформації або комп'ютерної системи має легальну мету у тому разі, коли програмна складова може функціонувати лише в цьому конкретному технічному середовищі (лише на цьому «залізі»). Така ситуація можлива, якщо ідентифікаційні дані технічного пристрою (чіп, процесор, матриця тощо) вбудовані в програмний код та є умовою розгортання системи (відомі приклади реалізації щодо фінансових програм підприємств для унеможливлення їх запуску на іншому технічному обладнанні у разі вилучення носія інформації з програмним кодом та даними підприємства). Також на практиці виявляються випадки, коли за результатами виготовлення криміналістичної копії носія інформації остання повністю не відбиває структуру даних, що відображаються на первинному пристрої. Вказане має місце при копіюванні даних деяких месенджерів, коли в структурі листування не відображаються окремі складники (зокрема, переслані повідомлення з інших

чатів) або програмні особливості додатка не дозволяють скопіювати таке листування з можливістю адекватного відтворення. Однак таку ситуацію повинен встановити фахівець під час огляду носія інформації або комп'ютерної системи і вказати у своєму письмовому висновку. Лише тоді, на нашу думку, з'являється легальна підстава утримання цього цінного носія інформації чи комп'ютерної системи з огляду на його технічну невід'ємність від інформації. Вибуття з володіння органу досудового розслідування відповідного технічного елементу може призвести до втрати інформації чи її частини або унеможливлення її відтворення й подальшого використання як доказу в кримінальному провадженні. Тоді на це майно (носій інформації, технічний пристрій, комп'ютерну систему тощо) може бути встановлено правовий режим, що передбачає обмеження права власності в частині володіння та користування – арешт майна. У такому разі визначення речовим доказом цінних носіїв інформації або комп'ютерних систем хоч і є вимушеним кроком на шляху реалізації процесуальної процедури арешту майна, має технічні та нормативні підстави [115, с. 85-92].

Непоодинокую є практика визначення речовими доказами всіх без винятку носіїв інформації в кримінальному провадженні, в тому числі CD-дисків з даними, що отримані за результатами тимчасового доступу до речей і документів у частині відомостей від операторів телекомунікацій, а також DVD-дисків з відеозаписом обшуку), що є нонсенсом. Останнє призводить лише до зобов'язання демонстрації стороні захисту оригіналів цих носіїв інформації під час відкриття матеріалів кримінального провадження в порядку ст. 290 КПК України – як речових доказів, а не надання доступу до копій інформації, що на них зберігається – як документів. Це створює ризики недобросовісної поведінки окремих представників сторони захисту щодо умисного пошкодження носіїв інформації з метою знищення доказів, що подекуди зустрічається на практиці [115, с. 85-92].

Серед процесуальних джерел доказів, передбачених ч. 2 ст. 84 КПК України, показання посідають важливе місце з огляду на їх обсяг, змістову насиченість та багатофункціональність інформації, яку вони можуть містити.

Тему показань як джерела доказів у кримінальному процесі України на дисертаційному рівні досліджували О. Д. Нарійчук (2012) [177], О. Г. Дехтяр (2014) [68], О. П. Острійчук (2016) [182], В. М. Лушпійченко (2018) [162], О. О. Сольонова (2018) [252] та ін. У процесі поступової цифровізації кримінального провадження показання як джерело доказів дедалі частіше набувають електронної форми. Це обумовлено не лише розвитком технічних засобів фіксації, а й необхідністю адаптації процесуальних інструментів до умов воєнного стану, обмеженого доступу до місця допиту, а також зростанням вимог до оперативності й збереження доказової інформації.

Застосування відеозапису під час допиту не лише забезпечує фіксацію змісту наданих показань, а й дозволяє закріпити контекст їх проголошення — поведінку особи, інтонацію, логічну структуру відповіді, емоційну виразність, що можуть бути предметом подальшого аналізу з боку суду або експерта. Таким чином, відеозапис показань виконує функцію гаранта достовірності змісту повідомленої інформації, зменшуючи ризики перекручення при подальшому відтворенні.

У чинному КПК України існують два механізми використання під час судового розгляду як доказу показань, що мають електронну форму (попри засаду безпосередності дослідження доказів судом), а саме: ст. 225 КПК України регламентує проведення допиту під час досудового розслідування в судовому засіданні – у виняткових випадках, через існування небезпеки для життя і здоров'я особи, її тяжкої хвороби, наявності інших обставин, що можуть унеможливити її допит в суді або вплинути на повноту чи достовірність показань; ч. 11 ст. 615 КПК України регламентує використання як доказів у суді показань, отриманих під час допиту свідка, потерпілого, у тому числі одночасного допиту двох чи більше вже допитаних осіб, у кримінальному провадженні, що здійснюється в умовах воєнного стану, якщо хід і результати такого допиту фіксувалися за допомогою доступних технічних засобів відеофіксації. Це має особливе значення в умовах цифровізації інституту доказування, коли первинним джерелом може стати не особа, а відеозапис, автентичність та цілісність якого має бути належно підтверджена.

Не вдаючись до наукової дискусії про вимоги до оформлення протоколу допиту, доцільно вказати на обставини, які слід врахувати при складанні процесуального документа, що відображає хід і результатів допиту, котрий фіксувався за допомогою технічних засобів відеофіксації. Такий протокол, окрім положень, що визначені ч. 3 ст. 104 КПК України, повинен містити: дані про особу, яка допитується, з вказівкою на спосіб її ідентифікації, а також, за наявності, програмні й технічні засоби, що були для цього використані; відомості про програмні та технічні засоби, що застосовувалися під час допиту; відомості про результати фіксації процесуальної дії (відеозапис), спосіб їх ідентифікації та підтвердження цілісності (за наявності); підпис особи, яка давала показання (включаючи, за потреби, електронний підпис).

Відповідно до ч. 2 ст. 104 КПК України у разі фіксування процесуальної дії під час досудового розслідування за допомогою технічних засобів про це зазначається у протоколі. Якщо за допомогою технічних засобів фіксується допит, текст показань може не вноситися до відповідного протоколу за умови, що жоден з учасників процесуальної дії не наполягає на цьому. У такому разі у протоколі зазначається, що показання зафіксовані на носії інформації, який додається до нього. При цьому згідно з ч. 3 ст. 107 КПК України у матеріалах кримінального провадження зберігаються оригінальні примірники технічних носіїв інформації зафіксованої процесуальної дії, резервні копії яких зберігаються окремо.

Отже, у разі застосування технічних засобів фіксації обов'язковим є зберігання носія інформації з результатами фіксації допиту як додатку до протоколу, з дотриманням вимог цілісності та незмінності.

Для виокремлення показань як доказу електронної форми, важливим є розуміння їх технічної природи. У разі відеофіксації або допиту з використанням відеозапису, первинним носієм доказової інформації є файл, що містить запис (відео або аудіо) із відповідними метаданими: датою, часом, геолокаційними даними, а також цифровим ідентифікатором пристрою, з якого здійснювався запис. Такий запис зберігається на електронному носії інформації, що підлягає

опечатуванню і повинен бути належно ідентифікований у матеріалах кримінального провадження.

Окрім того, у разі створення протоколу допиту в електронній формі (як електронного документа) необхідно враховувати вимоги Закону України «Про електронні документи та електронний документообіг»: обов'язковим елементом такого протоколу, поміж іншого, є наявність КЕП особи, яка проводила допит, а також — за можливості — підпису допитуваного.

Також варто вказати на особливості використання відеозв'язку дистанційного допиту, визначені в ч. 1 ст. 232 КПК України. Ця форма допиту передбачає, що технічні засоби і технології повинні забезпечувати належну якість зображення і звуку, а також інформаційну безпеку (ч. 3 ст. 232 КПК України). Водночас практика проведення допитів в режимі відеоконференції виявляє низку невирішених проблем, зокрема: технічні збої чи перешкоди в передачі сигналу (наприклад, Постанова ВС від 01.04.2025 у справі № 629/166/19); складнощі у фіксації процесу вручення пам'ятки про права або попередження про відповідальність у віддаленому форматі (ч. 5 ст. 232 КПК України частково вирішує це питання в організаційному аспекті); відсутність єдиних підходів до захисту відеозапису від зміни чи втрати. Ці аспекти вказують на необхідність подальшої процесуальної уніфікації та технічного доопрацювання дистанційної форми отримання показань з огляду на необхідність забезпечення їх цілісності.

Електронна форма фіксації показань має переваги та ризики. Серед переваг варто вказати: 1) електронна форма дозволяє зменшити ризики спотворення інформації (людський чинник); 2) забезпечується оперативність точного відтворення показань у будь-який момент провадження, незалежно від місцезнаходження допитаного; 3) використання технічних засобів фіксації створює умови для об'єктивної оцінки доказів, у тому числі шляхом залучення експертів до аналізу відеозапису на предмет поведінкових ознак брехні або тиску; 4) електронна форма фіксації показань сприяє забезпеченню їх збереження тривалий період, звісно, за умови належного захисту носіїв інформації.

Разом із перевагами електронна форма фіксації показань створює низку нових викликів: 1) можливість несанкціонованого втручання у цифрові носії інформації — редагування, монтаж, підміна або видалення фрагментів відео. У цьому контексті важливим є забезпечення криптографічного захисту відеозаписів, фіксація контрольних геш-кодів, ведення журналу доступу до файлів тощо; 2) автентифікація особи, яка надає показання в умовах дистанційного допиту. Без використання біометричних систем або КЕП ідентифікація може бути ускладнена, що створює простір для маніпуляцій; 3) стандартизація зберігання та подання показань, що мають електронну форму. Дотепер немає уніфікованого порядку щодо формату, обсягу, строку зберігання, порядку передачі або надання в суді відеозаписів допитів, що спричиняє фрагментарність практики та нерівномірність її застосування у різних регіонах; 4) практика фіксації показань за допомогою не сертифікованих технічних засобів. Це створює суттєві ризики, оскільки суд часто не має можливості встановити походження відеозапису, обставини його створення, а також гарантії того, що його зміст не зазнав змін.

Описані ризики зумовлюють деякі правозастосовні проблеми, зокрема — відсутність належного правового регулювання, що визначало б критерії оцінки показань, що мають електронну форму, адже первинним джерелом є не безпосередньо людина, а аудіо- або відеофайл. Дуже часта ситуація, коли сторони не мають уніфікованого доступу до оригіналів електронних носіїв або коли такі носії не містять метаданих чи геш-значень, що дозволяють підтвердити їх автентичність, незмінність і зв'язок із конкретною процесуальною дією. У багатьох випадках захист обґрунтовано заявляє клопотання про визнання таких доказів недопустимими, посилаючись на неможливість перевірки цілісності носія, автентичності підписів або відсутність належного протоколювання ланцюга передачі відеофайлу (chain of custody).

Також варто зауважити про необхідність удосконалення законодавчого регулювання. Наявні виклики свідчать про потребу вдосконалення нормативної бази щодо використання показань в електронній формі. Передусім потребує оновлення інститут технічної фіксації слідчих (розшукових) дій, зокрема шляхом

деталізації змісту ст. 107 КПК України в частині: визначення мінімального переліку метаданих, що мають супроводжувати файл із відеозаписом показань; обов'язкової верифікації особи, яка дає показання, із зазначенням методу та технічного засобу її ідентифікації; запровадження рекомендації щодо фіксації контрольної геш-суми відеозапису допиту.

Крім того, у перспективі слід розглянути можливість використання цифрових платформ для зберігання показань, що мають електронну форму (зокрема, у формі відеозаписів), які б забезпечували: резервне збереження файлів; захист від редагування; можливість перегляду усіма сторонами провадження; формування журналу доступу до запису.

Такий підхід дозволить створити прозору, контрольовану і юридично захищену систему фіксації й обігу показань, що мають електронну форму, та забезпечить рівність сторін у доступі до джерел доказування.

Отже, системний аналіз правової природи показань як джерела доказів у контексті їх фіксації в електронній формі свідчить про сутнісну трансформацію цього інституту. В електронній формі показання зберігають свої класичні ознаки — особистісний характер, обмежену об'єктивність, залежність від психологічного стану та добросовісності особи, яка їх надає. Водночас електронний спосіб фіксації змінює їх процесуальну оболонку, породжуючи нові вимоги до автентифікації, зберігання, подання та оцінки такого доказу.

З урахуванням вищезазначеного, можна констатувати, що показання в електронній формі мають потенціал перетворитися на ефективний, надійний та юридично захищений інструмент доказування. Для цього пропонується забезпечити: законодавче унормування технічних процедур їх фіксації, верифікації та інтеграції в кримінальний процес; технічне оновлення базової інфраструктури фіксації та обробки доказів; професійну підготовку суб'єктів доказування до роботи з показаннями, що мають електронну форму; уніфікацію судової практики, орієнтованої на сучасні технології й принципи цифровізації процесу доказування. Таким чином, електронна форма показань є не лише відповіддю на цифрові трансформації суспільства, але й стимулом для подальшого вдосконалення

національної моделі кримінального процесу України в бік прозорості, ефективності та технологічної стійкості.

Одним із проявів цифровізації кримінального процесу України є поступова еволюція такого класичного процесуального джерела доказів, як висновок експерта, із суто паперової форми до електронної. Практика вже сьогодні демонструє зростання кількості випадків оформлення висновку експерта як електронного документа, засвідченого електронним підписом. Водночас, попри наявність законодавчої бази, що допускає використання електронних документів у кримінальному провадженні, процес долучення та дослідження висновку експерта, що має форму електронного документа, в розумінні ч. 1 ст. 5 Закону України «Про електронні документи та електронний документообіг» залишається фрагментарним і методологічно не уніфікованим.

Тему висновку експерта як джерела доказів у кримінальному процесі України на дисертаційному рівні досліджували В. Д. Юрчишин (2006) [298], І. В. Пиріг (2006) [190], М. Г. Щербаковський (2016) [296], А. Р. Воробчак (2019) [36]. А. В. Столітній (2019) досліджує сучасний стан та перспективи розвитку електронної форми висновку експерта в кримінальному провадженні [259, с. 102-111]. М. Вілінський (2023) досліджує нормативні основи і практичні аспекти використання електронної форми висновку експерта в цивільному судочинстві [33, с. 14].

Практика правозастосування свідчить, що таке процесуальне джерело доказів у кримінальному провадженні, як висновок експерта, поступово трансформується з виключно паперового формату в електронний і вимагає формування чітких підходів та правил.

Передусім необхідно дослідити нормативні засади для використання висновку експерта, що має форму електронного документа, під час кримінального провадження. Відповідно до ч. 7 ст. 101 КПК України, висновок експерта надається в письмовій формі, але кожна сторона має право звернутися до суду з клопотанням про виклик експерта для допиту під час судового розгляду для роз'яснення чи доповнення його висновку (термін «письмовий» не тотожний термінові

«паперовий» і може мати як фізично надрукований чи написаний, так і електронний формат.

Частиною 1 ст. 5 Закону України «Про електронні документи та електронний документообіг» визначено, що електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа. Щодо обов’язкових реквізитів висновку експерта, то ч. 3 ст. 102 КПК України передбачає, що висновок підписується експертом, для чого може використовуватися електронний підпис (а саме – для ідентифікації автора електронного документа). При цьому юридична сила електронного документа та його допустимість як доказу не може бути заперечена виключно через те, що він має електронну форму (ч.ч. 1, 2 ст. 8 Закону України «Про електронні документи та електронний документообіг»). Щодо підзаконних НПА, то 24 червня 2022 р. набрав чинності наказ від 21.06.2022 р. № 2578/5 Міністерства юстиції України [223, с. 1], що доповнив розд. IV Інструкції про призначення та проведення судових експертиз й експертних досліджень, затвердженої наказом від 08.10.1998 № 53/5 Міністерства юстиції України, новим п. 4.22 [90, с. 1]. Із 24 червня 2022 р. експерти мають право викладати свій висновок в електронній формі і надавати такий суду чи заінтересованій особі [33, с. 14]. Вказане дозволяє стверджувати про хороші перспективи широкого впровадження електронного формату висновків експерта під час кримінального провадження з огляду на наявність відповідної нормативної бази та очевидні переваги збереження часу та матеріальних ресурсів.

На сьогодні цей процес під час досудового розслідування реалізовано на практиці через призму норм Закону України «Про електронні документи та електронний документообіг», що виражається у виготовленні висновку експерта як електронного документа – електронного файлу та його підписання шляхом накладання електронного підпису. Такий висновок експерта, що має форму електронного документа, передається до органів досудового розслідування та органів прокуратури за допомогою інформаційних систем, що забезпечують електронний документообіг у відповідних відомствах, надходить до слідчого або прокурора й долучається ними до матеріалів кримінального провадження. Наразі

практика правозастосування не є однорідною в цьому питанні, однак таке долучення часто відбувається шляхом друку відповідного електронного документа (на папері) та його долучення (підшивання) до матеріалів кримінального провадження. Другим шляхом є долучення і паперового відображення висновку експерта, що має форму електронного документа (описаного попередньо), і, також, носія інформації, на який завантажено файл відповідного електронного документа (яким є висновок експерта) та файл для перевірки справжності КЕП, яким він підписаний. Наведена практика ситуативно сформована суб'єктами правозастосування і не має чіткої нормативної регламентації [96, с. 87-88].

Але варто виявити і ризики, що можуть виникнути в досліджуваному питанні, дослідити їх для врахування слідчими й прокурорами та недопущення під час досудового розслідування. Насамперед, існують ризики при долученні до матеріалів кримінального провадження паперового відображення висновку експерта, що має форму електронного документа [96, с. 88]. Норми закону не виключають можливість використання паперового відображення висновку експерта, що має форму електронного документа (ч. 3, ч. 4 ст. 5 Закону України «Про електронні документи та електронний документообіг»).

Долучення до матеріалів кримінального провадження лише паперового відображення висновку експерта, що має форму електронного документа, хоч і допустиме з огляду на норми ч. 4 ст. 5 Закону України «Про електронні документи та електронний документообіг», однак не дозволяє перевірити цілісність та достовірність відповідного доказу.

Також потрібно звернути увагу на те, що згідно з ч. 2 ст. 7 Закону України «Про електронні документи та електронний документообіг», у разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Отже, оригіналів висновку експерта може бути одразу кілька. Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі

відображення, в тому числі у паперовій копії (ч. 4 ст. 7 Закону України «Про електронні документи та електронний документообіг»). Тобто повинен бути доступний файл, що дозволить здійснити перевірку справжності КЕП, яким підписаний відповідний висновок експерта.

Отже, по-перше, до матеріалів кримінального провадження необхідно долучати не лише паперове відображення висновку експерта, що має форму електронного документа, а й сам електронний файл, а також файл для перевірки КЕП; по-друге, на всіх етапах кримінального провадження (наприклад, прокурору при погодженні повідомлення про підозру чи обвинувального акта) доцільно здійснювати перевірку цілісності електронного файлу, яким є висновок експерта, що має форму електронного документа, а також справжності КЕП, яким він підписаний.

Наступним питанням є вимоги до електронного підпису, перевірки його справжності та вимог до учасників кримінального провадження щодо вчинення таких дій. У п. 15 ч. 1 ст. 1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» визначено, що електронний підпис – електронні дані, що додаються до інших електронних даних або логічно з ними пов'язуються і використовуються підписувачем як підпис. Відповідно до ч. 1 ст. 7 Закону України «Про електронні документи та електронний документообіг» оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги».

Однак для завдань кримінального провадження необхідно враховувати норму ч. 6 ст. 18 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», відповідно до якої КЕП має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису. Пунктом 27 ч. 1 ст. 1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» визначено, що КЕП – це удосконалений електронний підпис, що створюється з використанням засобу КЕП і базується на

кваліфікованому сертифікаті електронного підпису. Тобто для використання під час кримінального провадження електронні документи (в розумінні ч. 1 ст. 5 Закону України «Про електронні документи та електронний документообіг») загалом та зокрема висновок експерта, що має форму електронного документа, має бути підписано не електронним підписом, а саме КЕП.

Надзвичайно важливим аспектом є дослідження судом такого доказу. Під час судового розгляду кримінального провадження може постати питання про дотримання засади безпосередності дослідження показань, речей і документів (ст. 23 КПК України) та дослідження саме оригіналу висновку експерта, що має форму електронного документа. При визначенні засад дослідження показань, речей і документів ч. 1 ст. 23 КПК України передбачено, що суд досліджує докази безпосередньо, але особливості дослідження висновку експерта не визначені.

На нашу думку, під час судового розгляду кримінального провадження суд міг би обмежитися дослідженням паперового відображення такого електронного висновку експерта, якщо сторона захисту не заперечуватиме проти цього. Якщо ж сторона захисту висловлюватиме сумнів щодо цього питання, то варто врахувати вимоги ч. 1 ст. 7 Закону України «Про електронні документи та електронний документообіг», відповідно до яких оригіналом електронного документа вважається саме електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги», а не його паперове відображення. Тобто вимога щодо дослідження висновку експерта у формі електронного примірника документа, а не лише його відображення, таки має сенс. Тож суд мав би це враховувати, а процес дослідження судом висновку експерта, що має форму електронного документа, має передбачати вивчення саме електронного примірника висновку експерта (електронного файлу), перевірку цілісності файлу та справжності КЕП [96, с. 89].

Отже, у разі ініціювання стороною захисту відповідного питання під час судового розгляду кримінального провадження постане потреба саме в

електронному примірнику висновку експерта, що має форму електронного документа, який, як свідчить практика правозастосування, долучається до матеріалів кримінального провадження не завжди. Тобто постає питання про його долучення, що могло б відбуватися шляхом: а) надсилання слідчим або прокурором, який отримав такий файл, електронними засобами зв'язку, бажано відомчими; б) долучення слідчим або прокурором, який отримав такий файл, на носії інформації; в) витребування судом такого електронного файлу від експерта, що проводив відповідне дослідження, який надасть його на носії інформації або передасть засобами зв'язку. У цьому разі, на нашу думку, не варто вести мову про ризики визнання таких доказів недопустимими, а радше про потребу вчинення судом додаткових дій та витрати часу, що, однак, також не сприяє швидкому та ефективному судовому розгляду кримінального провадження.

Щодо процедур зберігання носіїв інформації з висновком експерта, що має форму електронного документа, варто вказати таке. Зберігання кількох висновків експерта на кількох носіях корелюється з поточною практикою, однак є недоцільним. У разі коли це не просто дані, а саме документи, що підписані КЕП, з метою економії ресурсів у одному кримінальному провадженні допустимо зберігати всі електронні документи (у розумінні ч. 1 ст. 5 Закону України «Про електронні документи та електронний документообіг») на одному носії інформації [96, с. 90]. Гешування таких електронних файлів для забезпечення підтвердження їх цілісності, на нашу думку, є недоцільним, адже технологія КЕП включає в себе процедури обрахування контрольних сум, що подібні до процедур, що використовуються під час гешування й забезпечують підтвердження цілісності даних аналогічного рівня.

Для забезпечення належного процесуального оформлення висновку експерта, що має форму електронного документа, доцільним є запровадження чітко визначеного алгоритму його долучення до матеріалів кримінального провадження. Першим етапом виступає створення електронного висновку експертом відповідно до вимог законодавства з накладенням КЕП та кваліфікованої електронної печатки установи (у разі наявності). Наступним кроком має бути отримання такого

висновку експерта уповноваженим суб'єктом (слідчим, прокурором тощо) та перевірка КЕП уповноваженою службовою особою органу досудового розслідування або прокуратури із фіксацією результатів такої перевірки (наприклад, у вигляді акту або службової записки). На завершальному етапі здійснюється долучення електронного висновку експерта до матеріалів кримінального провадження як у вигляді його паперового відображення, так і у формі електронного примірника (файлу) разом із файлом для перевірки КЕП — шляхом приєднання на відповідному електронному носії інформації (DVD-диск, USB-накопичувач тощо) із зазначенням цього факту у відповідному процесуальному документі (наприклад, у постанові або протоколі). Запровадження такого алгоритму дозволить забезпечити достовірність, цілісність і допустимість висновку експерта, що має форму електронного документа [96, с. 90-91].

Цифровізація суспільних процесів зумовила зміну не лише об'єктів та джерел доказів, а й саму її фізичну природу. У сучасних умовах лівова частка фактів, що мають значення для кримінального провадження, утворюється, створюється, передається, фіксується, зберігається та обробляється не в матеріальному середовищі, а в цифровому — у вигляді структурованих наборів даних, функціонально пов'язаних з апаратно-програмним середовищем. Така форма існування доказів принципово відрізняється від традиційної й обумовлює потребу в осмисленні їх технічної природи.

Технічна природа доказу електронної форми, є визначальною для розуміння його автентичності, цілісності, стабільності та здатності до відтворення під час кримінального провадження. Однак правове регулювання не охоплює технічну складову, що є подекуди визначальною для встановлення допустимості й достовірності доказів.

У цьому підрозділі спробуємо провести комплексний аналіз технічної природи процесів, пов'язаних з доказами електронної форми. З цією метою розкриємо їх ключові технічні характеристики, класифікацію електронних носіїв інформації для завдань кримінального провадження, здійснимо розмежування між логічним копіюванням даних та криміналістичним (побітовим) копіюванням носія

інформації, а також окреслимо природу геш-функцій як інструмента підтвердження цілісності доказу електронної форми.

Технічні властивості доказів електронної форми є важливою складовою, що підлягає встановленню та оцінці під час кримінального провадження. Доказ електронної форми, в розумінні бітової послідовності даних, не існує як самостійний матеріальний об'єкт – його фізична присутність в кримінальному провадженні реалізується лише через електронний носій інформації, на якому його збережено.

Нематеріальний характер бітової послідовності даних потребує матеріального носія інформації, що виконує функцію контейнера, який сам не є доказом, якщо не має характеристик, що має значення для доказування. У цьому контексті варто погодитися позицією Д. М. Цехана [283, с. 257], що суть документа визначається не матеріальним об'єктом – носієм інформації, а інформацією, яка на ньому зафіксована. Інформація також може існувати у кіберпросторі, бути розміщеною на віддалених серверах або зберігатися одночасно на кількох пристроях, не втрачаючи при цьому своєї значущості.

Однією з ключових технічних властивостей такого доказу є здатність до модифікації без очевидних ознак втручання. На відміну від матеріальних об'єктів, зміна цифрових (комп'ютерних) даних не завжди залишає помітні сліди, що можливо виявити без застосування спеціалізованих інструментів. Це створює ризики маніпулювання доказами. Відображення доказів в електронній формі здійснюється за допомогою програмних та технічних засобів, що забезпечують декодування цифрової інформації та її подання у візуалізованій формі, придатній для сприйняття людиною.

Таким чином, доказ електронної форми, суттєво залежить від технічного контексту свого існування, тож його значення для доказування обумовлюється не лише змістом інформації, а й за умовами створення, обробки та візуалізації.

Електронні пристрої, що можуть виступати доказами у кримінальному провадженні, мають багаторівневу внутрішню структуру, розуміння якої є

необхідною умовою для правильного аналізу змісту даних, перевірки достовірності та підтвердження цілісності.

Внутрішня структура доказу електронної форми, є 4-рівневою і включає: 1) контент – інформаційне ядро, що містить фактичні дані, які мають значення для кримінального провадження. Це може бути текстова, графічна, аудіо-, відеоінформація, дані журналів активності тощо. Контент становить змістову частину доказу, проте самостійно не забезпечує повноти доказового аналізу без урахування супровідних технічних параметрів; 2) метадані – виконують функцію технічної ідентифікації цифрового об'єкта. Вони можуть містити відомості про час створення, модифікації, доступу, розмір, формат, авторство, місце зберігання та інші характеристики контенту. Саме метадані дозволяють відтворити «історію» цифрового об'єкта, ідентифікувати джерело його походження та виявити втручання або спроби модифікації. У певних випадках метадані мають самостійне значення для доказування; 3) системна оболонка — це службова інформація операційної системи (програмного середовища), в межах яких існує цифровий об'єкт. Вона включає структуру директорій, атрибути файлової системи, тимчасові файли, системні журнали та інші автоматично створювані програмним середовищем компоненти. Системна обгортка є контекстом для інтерпретації як контенту, так і метаданих, а також відіграє важливу роль у процесі підтвердження цілісності доказу; 4) носій інформації – фізичний об'єкт, що забезпечує фізичне існування та зберігання доказу електронної форми.

Також варто визначити деякі особливості комп'ютерних пристроїв. Зокрема, комп'ютерна система містить апаратне та ПЗ, які обробляють дані й охоплюють, зокрема: контейнер, який містить плати, мікропроцесори, жорсткий диск, пристрої пам'яті та інтерфейсні підключення; монітор або відеодисплей; пристрої зберігання даних: жорсткі диски; зовнішні жорсткі диски; знімні носії; флеш-накопичувачі; карти пам'яті; портативні пристрої; периферійні пристрої; інші пристрої; комп'ютерні мережі [24, с. 116–117].

Дедалі активніше використання сучасних ІТ та ЕНІ в контексті кримінальних процесуальних процедур обумовлює напрацювання процесуально та технічно

коректного алгоритму роботи з доказами, що обумовлює необхідність коректного підходу до класифікації електронних носіїв інформації та інформаційних систем для забезпечення виконання завдань кримінального провадження [112, с. 211].

За власником та основним користувачем дослідники поділяють електронно-обчислювальну техніку на: особисту, або персональну електронно-обчислювальну техніку; мережеві накопичувані інформації; спільну електронно-обчислювальну техніку.

КПК України ілюструє своєрідний «вулик» термінів з досліджуваного питання, зокрема: «електронний документ» (ч. 3 ст. 99, ч. 5 ст. 106-1), «електронні інформаційні системи» (п. 4 ч. 4 ст. 258, ст.ст. 264–265), «електронні інформаційні системи або їх частини» (абз. 2 ч. 1 ст. 159, ч. 2 ст. 168), «інформаційні (автоматизовані) системи» (ч. 4 ст. 99, абз. 4 ч. 2 ст. 168), «інформаційно-телекомунікаційні системи» (ч. 4 ст. 99), «інформаційно-телекомунікаційні системи, їх невід’ємні частини» (абз. 4 ч. 2 ст. 168), «інші носії інформації (у тому числі електронні)» (п. 1 ч. 2 ст. 99), «мобільні термінали систем зв’язку» (абз. 2 ч. 1 ст. 159), «носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії» (п. 3 ч. 2 ст. 99), «радіоелектронні засоби» (ст. 268), «телекомунікаційні системи» (ч. 4 ст. 99, абз. 4 ч. 2 ст. 168). Всі ці терміни так чи інакше пов’язані з процесом збирання доказів. Первинне збирання доказів електронної форми під час досудового розслідування у більшості випадків проводиться з електронних носіїв інформації, які стають фізично доступними слідчому, прокурору під час проведення слідчих (розшукових) чи інших процесуальних дій, зокрема: обшуку, огляду, тимчасового доступу до речей і документів тощо.

Об’єктом пошуку стає електронний носій інформації, на якому зберігається власне цифрові (комп’ютерні) дані, що цікавлять сторону обвинувачення, та потенційно є доказом. Таким чином, ключовим у даному питанні стає сам електронний носій інформації (відокремлений або вбудований). Але термін «електронний носій інформації» нормативно не визначено ні в КПК України, ні в профільному законодавстві [112, с. 212].

Водночас ДСТУ 7448:2013 визначає електронний носій як матеріальний носій, який використовують для записування, зберігання та відтворення інформації, обробленої засобами комп'ютерної техніки. До електронних носіїв відносяться жорсткі диски, флеш-пам'ять, CD, DVD, Blue-ray, диски дискети, касети на магнітній стрічці і та ін. [80].

Релевантна класифікація електронних носіїв інформації є передумовою для уніфікації процедур їх виявлення, вилучення, зберігання та дослідження а також адаптації процесуальних дій до технічних особливостей цифрового середовища.

Ілюстративний перелік типових електронних носіїв інформації включає: персональні пристрої, до яких найчастіше належать смартфони, ноутбуки та планшети; периферійні носії — це окремі модулі зберігання інформації, що підключаються до основних пристроїв, до яких належать флеш-накопичувачі, зовнішні жорсткі диски, карти пам'яті тощо. Серед різновидів носіїв інформації окреме місце посідають пристрої Інтернету речей; мережеві та віртуальні середовища, що охоплюють маршрутизатори, о фіксують мережеву активність і містять журнали з'єднань; сервери, хмарні сховища, сервери месенджерів а також віртуальні машини.

Наведена класифікація ілюструє, що цифровий простір, у межах якого виникають, створюються та існують докази в електронній формі, є багаторівневим і технічно гетерогенним. Тому залежно від особливостей цифрового середовища електронні носії інформації для завдань кримінального провадження в частині збирання доказів електронної форми доцільно класифікувати за такими критеріями:

I. За доступністю доцільно виділяти:

1) Локальні – це фізично доступні для суб'єкта кримінального провадження

I. За доступністю пристрої, що можуть бути оглянуті та, за потреби, вилучені (наприклад, ноутбук, смартфон, зовнішній диск тощо);

2) Віддалені носії – ті, що фізично знаходяться поза межами контролю суб'єкта кримінального провадження, але до яких є логічний доступ через мережеві

протоколи (наприклад, хмарне сховище, поштовий сервер, обліковий запис у сервісі обміну повідомленнями тощо);

3) Динамічні носії характеризуються тимчасовістю існування та генеруються в процесі активної мережевої взаємодії (наприклад, сесія обміну повідомленнями в реальному часі, IP-з'єднання, інтерактивний потік даних тощо).

II. За середовищем зберігання носії поділяються на:

1) Фізичні. До них належать матеріальні пристрої з елементами пам'яті (жорсткі диски, флеш-накопичувачі, маршрутизатори тощо);

2) Віртуальні носії функціонують у хмарних або ізольованих віртуалізованих середовищах — таких, як сервери в дата-центрах, контейнери або віртуальні машини, що фізично не локалізовані в межах досяжності суб'єкта кримінального провадження, однак містять дані, що мають значення для кримінального провадження.

III. За типом пам'яті:

1) Постійна пам'ять (наприклад, HDD, SSD) забезпечує збереження інформації навіть після вимкнення пристрою;

2) Тимчасова пам'ять (RAM, кеш) характеризується високою швидкістю доступу, але втрачає вміст після завершення роботи пристрою (втрати живлення) або сесії;

3) Розподілена пам'ять функціонує в межах децентралізованих систем, як-от P2P-мережі або блокчейн-платформи, де інформація реплікується на множині вузлів, що ускладнює її видалення й автентифікацію.

Кожен з наведених критеріїв має практичне значення для вибору технічних засобів і процесуальних рішень, що доцільно застосовувати при роботі з носіями інформації під час кримінального провадження.

Також залежно від технічної конструкції електронних носіїв інформації для завдань кримінального провадження в частині збирання доказів електронної форми доцільно класифікувати за такими критеріями:

I. Ступенем інтеграції електронного носія інформації з інформаційною системою (далі - ІС):

1) відокремлені від ІС. Електронний носій інформації стає доступним слідчому, прокурору як окремий пристрій, що безпосередньо призначений для зберігання електронної інформації. До таких пристроїв відносяться знімні носії – дискети, оптичні диски, карти пам'яті, USB флеш-накопичувачі, накопичувачі на жорстких магнітних дисках, твердотілі накопичувачі, стрічкові картриджі тощо. Вивчення інформації на такому електронному носії передбачає його безпосереднє підключення до комп'ютера для подальшого дослідження інформаційного наповнення.

2) вбудовані в ІС. Електронний носій інформації представлений у складі комп'ютера, мобільного телефона чи іншого виду інформаційної системи. Такі носії поділяються на такі, що: а) можуть бути відокремлені (від'єднані) від ІС без втрати властивостей. Такі відносяться до знімних або дискретних, тобто можуть відокремлюватися від інформаційних систем (комп'ютерів, телефонів); б) можуть бути відокремлені (від'єднані) від ІС лише шляхом фізичного знищення стійких структурних елементів та порушення цілісності ІС. Існує велика кількість вбудованих або інтегрованих носіїв інформації, що неможливо відділити від системи без її пошкодження або суттєвого складного втручання. Носій інформації знаходиться всередині системи та не підлягає від'єднанню від системи без порушення її механічної цілісності. Наприклад, у складі мобільних телефонів, планшетних комп'ютерів та окремих ноутбуків основний модуль пам'яті є фізично інтегрованим компонентом, розпаяним на системній платі, і не може бути відділеним без порушення цілісності основного пристрою. У цьому разі доступ до електронного носія інформації для його вивчення відбувається через інтерфейси інформаційної системи, складовою частиною якої є цей носій.

II. Типом запам'ятовуючого пристрою:

1. Оперативний запам'ятовуючий пристрій – енергозалежна пам'ять. Оперативний запам'ятовуючий пристрій будь-якої інформаційної системи зберігає обмежену кількість електронної інформації лише протягом сеансу роботи системи до її вимкнення. В абсолютній більшості випадків увага спрямована слідчого спрямована на збирання інформації з енергонезалежних носіїв, хоча трапляються

випадки, коли інформація в оперативній пам'яті може становити суттєвий інтерес для слідства.

2. Енергонезалежний запам'ятовуючий пристрій (non-volatile storage) – енергонезалежна пам'ять, яка може зберігати інформацію при відсутності живлення, тобто після сеансу роботи системи та її вимкнення [112, с. 212–213].

Отже, коректна оцінка обстановки на місці проведення слідчих (розшукових) дій щодо виявлення та забезпечення стабільної роботи об'єктів, що потенційно містять електронні дані, виявлення електронних носіїв інформації та визначення його типу, а також коректна побудова алгоритму роботи з відповідними об'єктами, що потенційно містять електронні дані, є передумовою ефективного виявлення та фіксації доказів в електронній формі. Залежно від виду електронного носія інформації слідчому, прокурору під час проведенні слідчих (розшукових) дій необхідно забезпечити першочергове дослідження носіїв, інформація в яких може бути нестабільною, вживати заходів до забезпечення безперебійного живлення інформаційних систем для збереження інформації з оперативних запам'ятовуючих пристроїв. Окрім того, правильна класифікація електронних носіїв інформації за ступенем інтеграції з ІС може бути необхідна, наприклад, для обґрунтування необхідності арешту тимчасово вилученого майна або підтвердження позиції сторони обвинувачення при вирішенні питання про зняття арешту з майна та його повернення власнику [112, с. 213].

Кожен з видів електронних носіїв інформації потребує диференційованого підходу до виявлення та вилучення з урахуванням технічних характеристик, формату зберігання та рівня інтеграції в інфраструктуру. Ігнорування цих особливостей може призвести до втрати або спотворення даних. Відповідні питання врегульовано в ДСТУ ISO/IEC 27037:2017 [83, с. 1–31].

Метадані — це технічні атрибути цифрового об'єкта, що автоматично фіксуються операційною системою або програмним середовищем під час створення, зміни чи переміщення даних. Частина метаданих є незмінною, інші можуть бути модифіковані користувачем або стороннім програмним засобом.

Верифікація метаданих здійснюється через їх технічний аналіз із використанням спеціалізованого ПЗ. Надійність підвищується шляхом співставлення цих відомостей з іншими цифровими об'єктами — логами системи, журналами дій, записами мережевої активності. Такий підхід дозволяє виключити або підтвердити спроби навмисної фальсифікації.

Метадані мають значення для доказування, оскільки містять інформацію про час, місце, авторство та спосіб створення цифрового об'єкта. Це дозволяє встановити, чи відповідає технічна історія об'єкта змісту подій, на які вказують сторони кримінального провадження.

Метадані – це термін, який походить від англійського слова «metadata» (meta, грец. – «після», data, англ. – «інформація», «відомості», «дані») означає дослівно «дані про дані» [240, с. 50]. А. В. Гутник (Ратнова) переконана у необхідності використовувати термін «метадані», та додати можливість його дослідження в перелік орієнтованих питань експертизи [240, с. 51].

Метадані, як структуровані відомості про властивості, походження та зміну доказу електронної форми, мають суттєве значення для перевірки повноти, цілісності, а також допустимості доказу в кримінальному провадженні. Вони можуть фіксувати хронологію створення, доступу та модифікацій, а також інформацію про середовище походження даних. Водночас технічна природа метаданих обумовлює їх вразливість. Хоча пересічний користувач не має доступу до редагування системних атрибутів, досвідчені користувачі (особливо з профільними знаннями) за допомогою спеціалізованого ПЗ можуть модифікувати або знищити ці дані без слідів втручання. Метадані також можуть бути втрачені внаслідок технічного збою чи пошкодження носія.

Враховуючи зазначене, оцінка характеристик доказу електронної форми, виключно на підставі метаданих не забезпечує належних гарантій. Використання метаданих має ґрунтуватися на їх верифікації та співвіднесенні з іншими відомості про цифрові (комп'ютерні) дані, включно з аналізом цифрових слідів, журналів подій, геш-сум і технологічного середовища формування.

Автентичність цифрової інформації є базовою умовою її процесуальної допустимості. Будь-яке копіювання електронного носія інформації у межах кримінального провадження має відбуватися з урахуванням його технічної структури, оскільки цифрові дані позбавлені сталої фізичної форми та схильні до непомітної модифікації. У цьому контексті важливо розмежувати копіювання окремого файлу (логічне) та побітове (криміналістичне) копіювання носія інформації.

Логічне копіювання – це технічна операція відтворення змістовної частини цифрової інформації, яка здійснюється у межах файлової системи шляхом копіювання лише активних, доступних користувачу файлів, без відображення повного (низькорівневого) контексту їх існування. Такий спосіб охоплює імена файлів, розширення, вміст, а також частину атрибутів, проте не включає такі важливі для доказування елементи потенційного доказу електронної форми, як: метадані файлу, включно з точними мітками часу створення, останнього доступу та модифікації; службові таблиці, що відображають фізичну локалізацію даних на ЕНІ; фрагменти стертих або переміщених файлів, які можуть бути відновлені лише у межах первинного (або тотожного йому) носія; інформація з прихованих розділів, системного резерву або не підмонтованих томів. Цей технічний процес реалізується за допомогою операції «копіювати» та «вставити», використовуючи буфер обміну або комбінацію клавіш «Ctrl+C» та «Ctrl+V», або ж через контекстне меню. З огляду на це, використання методу логічного копіювання щодо доказу електронної форми, не забезпечує відображення структурної цілісності ЕНІ та середовища, в якому він існував, а лише окремого файлу(-ів).

Побітове копіювання носія інформації або ж створення криміналістичної (побітової) копії (образу носія інформації) є технічно значно складнішим.

Криміналістична (побітова) копія — це точна технічна репліка фізичної структури електронного носія інформації, що створюється шляхом побітового копіювання. Цей процес охоплює зчитування вмісту носія на секторному рівні, незалежно від наявності або видимості файлів у файловій системі. Під час описуваного процесу забезпечується повне збереження змістовної й технічної

інформації: метаданих, слідів цифрової активності, а також елементів файлової служби — зокрема таблиць розміщення файлів, як-от Master File Table (MFT) на NTFS. У копію також включаються дані з кошика, фрагменти частково стертих файлів, інформація з прихованих розділів, системних томів та вільного простору носія. Досліджуваний підхід дозволяє зберегти не лише видимий обсяг даних (як при логічному копіюванні), але й неактивні чи видалені фрагменти чи артефакти. Цим способом створюється *forensics images*, що є галузевим стандартом у цифровій криміналістиці.

При виготовленні копії конкретного файлу (логічному копіюванні) здійснюється копіювання конкретного блоку електронної інформації з визначеним ім'ям, розміром та атрибутами. У разі виготовлення криміналістичної (побітової) копії електронного носія інформації (далі – ЕНІ) копіюються послідовно всі інформаційні блоки носія інформації, що призначені для зберігання даних (від першого до останнього біта). Створення такої копії є створенням образу інформації з ЕНІ, що є тотожним оригінальному ЕНІ. Тобто, наприклад, при виявленні під час обшуку інформаційної системи з вбудованим ЕНІ загальною місткістю 64 гігабайти та записаною на ньому інформацією об'ємом 12 гігабайтів при копіюванні лише наявних файлів отримаємо 12 гігабайтів даних, а при виготовленні фізичної копії ЕНІ – 64 гігабайти. Крім того, при наступному дослідженні фізичної копії ЕНІ можливо відновити видалені електронні дані, що не виявлені первинним оглядом ЕНІ, який проведений лише в частині наявних файлів [125, с. 338]. Наведений приклад ілюструє важливість розуміння технічного аспекту роботи з електронними даними під час кримінального провадження та необхідність забезпечення систематичного навчання та підвищення кваліфікації слідчих, прокурорів щодо роботи з доказами електронної форми.

У кримінальному провадженні криміналістична копія є єдиним технічно обґрунтованим способом відтворення повного цифрового середовища, що забезпечує автентичність, повторюваність результатів аналізу та процесуальну допустимість отриманої інформації. Вона надає змогу зберегти стан носія

інформації на момент слідчої дії і дозволяє багаторазове дослідження без ризику зміни первинного об'єкта.

Для створення криміналістичних образів (фізичних або побітових копій) електронних носіїв інформації застосовуються спеціалізовані програмні засоби, що забезпечують зчитування даних на найнижчому рівні з одночасним контролем цілісності інформації та фіксацією відповідного технічного контексту. Такий підхід дозволяє відтворити не лише вміст файлів, але й службові структури файлової системи, включно з метаданими, залишковими даними (slack space), видаленими фрагментами та інформацією з непідмонтованих розділів.

Окрім ПЗ, при створенні криміналістичних копій має бути обов'язково використано апаратний write-blocker, який унеможливорює внесення змін до вихідного носія під час зчитування. Це є критично важливою умовою збереження автентичності оригінального джерела даних та дотримання вимог допустимості у кримінальному провадженні.

Таким чином, вибір інструментів копіювання має базуватись на стандартах збереження цілісності цифрових доказів, їх повторюваності та юридичній достовірності в умовах кримінального процесуального використання.

Отже, побітове копіювання носія інформації є оптимальним способом здобуття доказів щодо забезпечення їх цілісності під час кримінального провадження. Логічне копіювання фіксує лише доступні дані, що необхідно враховувати та релевантно застосовувати під час фіксації доказів.

Гешування – надійний метод підтвердження цілісності доказів електронної форми. П. 7.1.3.1.2 ДСТУ ISO/IEC 27037:2017 вказує на необхідність обчислення та документування геш-значень (рядок бітів, яка є виходом геш-функції) [83, с. 2, с. 21] потенційних цифрових доказів. Цей невідомий переважній більшості правників термін надає учасникам кримінального процесу унікальні можливості гарантування цілісності доказів в електронній формі [118, с. 73].

Геш-функція (геш та hash застосовуються в даній роботі як тотожні поняття – прим. авт.) являє собою функцію, математичну або іншу, що отримує на вхід рядок змінної довжини і перетворює його в рядок фіксованої, зазвичай меншої,

довжини. Такі перетворення ще називають функціями згортки, а їх результати – гешем, геш-значенням або дайджестом повідомлення. Алгоритм гешування – це послідовність математичних перетворень, в результаті яких з деякої двійкової послідовності змінної довжини отримується унікальна двійкова послідовність фіксованої довжини. Практично усі геш-функції працюють за одним і тим самим принципом. Вхідне значення (повідомлення, файл тощо) розглядається як послідовність n -бітних блоків. Кожен блок обробляється послідовно один за визначеним алгоритмом гешування, а в результаті обробки останнього блоку отримується m -бітове геш-значення [297, с. 86].

Якщо намагатися не вдаватися до складної технічної термінології, то гешування (hashing) можна охарактеризувати як технічний процес, заснований на математичному алгоритмі, що перетворює вхідні цифрові (комп'ютерні) дані (бітовий рядок даних, одиниці та нулі) у вихідний рядок даних фіксованого розміру (геш-значення або геш-суму).

Застосування геш-функцій : перевірка цілісності повідомлень та файлів – порівнюючи геш-значення повідомлень, обчислені до та після надсилання, можна визначити, чи були внесені будь-які зміни до повідомлення або файлу; верифікація пароля – паролі користувачів зберігаються у базі даних не у відкритому вигляді, а у вигляді гешів та не можуть бути відновлені зі збережених геш-значень; генерація і перевірка електронного підпису – обчислення гешу дозволяє виявити найменші зміни у документі та перевірити дійсність підпису [297, с. 86].

ДСТУ ISO/IEC 27037:2017 встановлює, що функції верифікації зазвичай застосовують з використанням геш-функцій, таких як MD5, SHA1 тощо, але може бути використано інші методи [83, с. 3]. SHA-256 є окремим випадком геш-функції із сімейства криптографічних геш-функцій SHA-2 (Secure Hash Algorithm Version 2), опублікованим АНБ США у 2002 році. У грудні 2014 року прийнято національний стандарт ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування» (введений в дію 1 квітня 2015 р.) [81], що базується на криптографічній функції гешування «Купина» [297, с. 88]. Ключовою для нас властивістю криптографічної геш-функції є відсутність

колізій (унікальність геша) [297, с. 87]. Це дозволяє виявити найменші зміни у комп'ютерних даних, тобто забезпечити підтвердження його незмінності та цілісності при збігові геш-значень в протоколі з геш-значеннями досліджуваних комп'ютерних даних, адже це свідчить про їх ідентичність на побутовому рівні [118, с. 74].

Ключовими характеристиками гешування є: незворотність – математична неспроможність обчислити первинні дані, маючи лише геш-значення. Це перетворення є одностороннім, тобто на основі геш-значення неможливо відновити початковий набір даних, відтак унеможливорює підробку геш-значення шляхом підбору змісту. детермінованість гарантує, що для однакових вхідних даних результат гешування завжди буде ідентичним, що дозволяє використовувати геш-значення як стабільний індикатор цілісності. унікальність (колізійна стійкість) передбачає, що ймовірність утворення однакового геш-значення для двох різних наборів даних є статистично мізерною.

У комп'ютерній криміналістиці заведено використовувати одnobічну геш-функцію як основну технологію, з використанням якої здійснюється ідентифікація комп'ютерних даних і перевіряється їх цілісність. Ця технологія дає змогу зафіксувати логічний (внутрішній) стан комп'ютерних даних будь-якої ємності через створення короткого цифрового відбитку (геш-коду), який можна письмово відтворити в документах.

Поділяємо позицію А. М. Гаркуші (2024), що для ідентифікації комп'ютерних даних у процесуальних документах та перевірки їх цілісності можуть бути використані як прості, так і сильні геш-функції. Актуальний перелік геш-функцій, які вважаються сильними, завжди може бути встановлений з офіційних документів. Такими геш-функціями сьогодні в Україні є SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256, SHA3-256, SHA3-384, SHA3-512, Купина-256, Купина-384, Купина-512 та GOST 34.311-95. Із часом сильні геш-функції можуть переходити до категорії простих. Якщо геш-функція втрачає ознаки, які зумовлюють її належність до виду простих геш-функцій, зокрема в разі винайдення алгоритму знаходження другого прообразу, її застосування для цілей ідентифікації

комп'ютерних даних може бути визнано неефективним. У виборі алгоритмів геш-функцій для застосування для ідентифікації комп'ютерних даних і перевірки їх цілісності рекомендується орієнтуватися на актуальний список сильних геш-функцій, причому використання лише одного алгоритму геш-функції вважається достатнім. Найпоширенішим сильним алгоритмом геш-функції сьогодення є SHA-256. У разі неможливості використати сильну геш-функцію в механізмах забезпечення цілісності даних слід розглянути питання про комбіноване застосування двох простих геш-функцій (наприклад, MD5 та SHA-1) або однієї простої геш-функції з максимально великою довжиною геш-коду (наприклад, слід надати перевагу алгоритму SHA-1, який продукує геш-код завдовжки 160 біт, перед алгоритмом MD5, який продукує геш-код завдовжки 128 біт) [41, с. 92].

Гешування під час кримінального провадження виконує функцію цифрового ідентифікатора об'єкта, що зафіксовано у конкретний момент часу. Будь-яка зміна, навіть мінімальна, у структурі або вмісті цифрового об'єкта змінює його геш-значення, що дозволяє точно встановити факт цілісності або його порушення. У кримінальному провадженні це надає можливість контролювати незмінність доказу електронної форми з моменту його вилучення до представлення й дослідження під час судового розгляду.

Отже, обрахування геш-сум комп'ютерних даних та їх фіксації в протоколі забезпечує підтвердження цілісності комп'ютерних даних на всіх стадіях кримінального провадження та має застосовуватися як спосіб ідентифікації комп'ютерних даних при виконанні вимог п. 3 ч. 3 ст. 104 КПК України [118, с. 74].

Пунктом 15 ч. 1 ст. 1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» визначено, що електронний підпис – електронні дані, що додаються до інших електронних даних або логічно з ними пов'язуються і використовуються підписувачем як підпис [227, с. 1]. Електронний підпис є ключовим інструментом аутентифікації в цифровому середовищі, що забезпечує юридичну значимість електронного документа та дозволяє підтвердити його походження, цілісність і авторство.

Чинним законодавством України передбачено три види електронного підпису: простий електронний підпис, удосконалений електронний підпис і КЕП. Простий електронний підпис не містить криптографічного захисту та не потребує залучення надавача довірчих послуг. Удосконалений електронний підпис створюється з використанням засобів, що забезпечують ідентифікацію підписувача та виявлення змін у документі після підписання, але не обов'язково ґрунтується на кваліфікованому сертифікаті. КЕП - удосконалений електронний підпис, що створюється з використанням засобу КЕП і базується на кваліфікованому сертифікаті електронного підпису (п. 27 ч. 1 ст. 1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги»).

Технологія створення електронного підпису передбачає використання криптографічного алгоритму з відкритим і закритим ключем, що утворює унікальний підпис шляхом математичної обробки геш-значення документа. Особистий (закритий) ключ, що перебуває виключно у володінні підписувача, генерує підпис, який може бути перевірений відкритим ключем через сертифікаційний центр. Процес автентифікації включає перевірку геш-значення документа, ідентифікацію підписувача через сертифікат та контроль цілісності даних. Указаний механізм уможливорює застосування електронного підпису в межах кримінального провадження як одного з елементів підтвердження автентичності та цілісності доказу електронної форми з огляду на використання під час його створення алгоритмів гешування.

Електронна позначка часу є важливим технічним і юридичним інструментом забезпечення достовірності моменту створення або підписання електронного документа. Відповідно до п. 13. ч. 1 ст. 1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», електронна позначка часу – це електронні дані, що пов'язують інші електронні дані з конкретним моментом часу для засвідчення наявності цих електронних даних на цей момент часу. Також п. 26. ч. 1 ст. 1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» визначає кваліфіковану електронну позначку часу як таку, що відповідає вимогам, встановленим ч. 2 ст. 26 цього Закону.

Кваліфікована електронна позначка часу повинна відповідати вимогам, визначеним ч. 2 ст. 26 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», що включає пов'язування дати і часу з електронними даними, що виключає можливість їх зміни без можливості виявлення, синхронізацію із Всесвітнім координованим часом (UTC) з точністю до секунди та інше. Кваліфікована електронна позначка часу має презумпцію точності дати та часу, на які вона вказує, та цілісності електронних даних, з якими ці дата та час пов'язані (ч. 1 ст. 26 Закону України «Про електронну ідентифікацію та електронні довірчі послуги») [227, с. 1].

Технологічно електронна позначка часу реалізується шляхом створення геш-функції об'єкта (файлу, документа тощо), яка надсилається на сервер довірчої служби, де фіксується разом із часовим штампом, генерованим на основі синхронізованих джерел точного часу. У відповідь користувач отримує сертифікований файл з унікальним ідентифікатором часу, що може бути використаний для перевірки моменту створення відповідного об'єкта.

У межах кримінального процесу електронна позначка часу може відігравати важливу роль у доведенні хронологічного порядку подій, оцінці достовірності джерела доказу електронної форми та перевірці відповідності chain of custody. Таким чином, вона є важливим елементом загальної системи забезпечення автентичності, цілісності та допустимості доказів електронної форми під час кримінального провадження.

А. М. Гаркуша (2025) досліджує питання використання кваліфікованої електронної позначки часу для фіксації комп'ютерних даних у кримінальному провадженні [42], що, безперечно, є перспективним напрямом для вдосконалення правозастосовної практики у відповідній сфері.

Цілісність означає незмінність технічної структури доказу електронної форми з моменту його фіксації під час досудового розслідування кримінального провадження. Будь-яке втручання у вміст або структуру такого виду доказу без належного контролю створює ризик його модифікації (зміни), що напряму впливає на процесуальну допустимість такого доказу. Відтак варто розглядати цілісність як

умову процесуальної допустимості доказу електронної форми. Підтвердження цілісності досягається шляхом обчислення та фіксації геш-значень, а незмінності – фіксацію chain of custody та використання належних програмних та технічних засобів (наприклад, використання write-blocker-пристроїв), які унеможливлюють зміну даних на оригінальному носії. Ці технічні рішення мають бути реалізовані на момент вилучення або першого доступу до доказу електронної форми.

У кримінальному провадженні, що включає роботу з доказами електронної форми відбувається об'єктивна взаємодія між технічними характеристиками об'єкта та юридичними критеріями його належності, допустимості й достовірності. Цифрова цілісність, що забезпечується через побітове копіювання та верифікується геш-функціями, становить не лише технічний параметр, але і процесуальну передумову допустимості доказу в контексті ст. 86 КПК України. Так само автентичність цифрового об'єкта як підтвердження його походження є передумовою належності доказу, тоді як достовірність базується на метаданих, що дозволяють реконструювати обставини створення, обробки та зберігання даних відповідно до вимог ст. 94 КПК України. Така взаємна детермінація технічного і юридичного рівнів вимагає чіткої формалізації у процесуальних стандартах, що в свою чергу забезпечує єдність підходів у практиці.

Особливу роль у забезпеченні техніко-юридичної інтеграції відіграє інститут chain of custody, який виконує функцію безперервного документального контролю за об'єктом від моменту його виявлення під час досудового розслідування кримінального провадження до використання в суді під час доказування обставин вчинення кримінального правопорушення. У цьому контексті chain of custody фіксує всі ключові параметри: збереження цілісності (геш-значення), підтвердження джерела (ідентифікація пристроїв і користувачів), збереження контексту (умови та носії) тощо. Його застосування дозволяє суб'єктам кримінального процесу (зокрема суду) перевірити відповідність кожної технічної операції процесуальним вимогам, забезпечуючи підтвердження цілісності даних.

У межах дослідження технічної природи доказів електронної форми необхідно виокремити групи об'єктів, що мають винятково цифрову природу,

тобто не є результатом фіксації аналогових процесів у цифровому форматі (як у разі з відеозаписами), не створені з метою збереження та відтворення інформації у формі, придатній для прочитання людиною (як текстові документи чи електронні таблиці), і не є електронним аналогом класичних носіїв інформації (як електронні документи відповідно до Закону України «Про електронні документи та електронний документообіг»).

Йдеться про об'єкти цифрової реальності, що виникають та функціонують виключно в цифровому середовищі, не маючи матеріального вираження чи відображення без їх цілеспрямованої фіксації. До таких об'єктів належать, зокрема: транзакції криптовалют, мережеві сесії доступу, цифрові сліди активності в інформаційних системах, RAM, лог-файли з обмеженим часом зберігання, елементи динамічного контенту (наприклад, змінний код сторінки вебсайту), дії ботів або віртуальних агентів тощо. Вони не зберігаються у вигляді сталих структурованих файлів, а існують як частина динамічної цифрової взаємодії.

Основною властивістю таких об'єктів є їх неспроможність до безпосереднього сприйняття чи перевірки в матеріальному вимірі без спеціальної фіксації (preservation) або збереження — як за ініціативою людини, так і шляхом автоматизованого захоплення комп'ютерною системою. У цьому контексті їх фіксація під час проведення слідчих (розшукових) дій або НСРД виступає єдиним способом переведення цих нестабільних об'єктів у доказово релевантну форму, що здатна бути інтегрованою у процес доказування.

Таким чином, у межах сучасного кримінального процесу об'єктивно можна вести мову про цифровий доказ не як про електронний документ або файл, а як про складні інформаційні об'єкти, що існують виключно в умовах цифрового середовища (кіберпростору), є інтерактивними, тимчасовими або змінними за своєю природою, і тому потребують спеціальних процедур збереження для набуття належного процесуального статусу. Це обґрунтовує необхідність їх виокремлення як самостійної процесуальної категорії, а також нормативного закріплення СОП щодо взаємодії з ними під час кримінального провадження.

РОЗДІЛ 2. ПРАКТИКА РОБОТИ З ДОКАЗАМИ ЕЛЕКТРОННОЇ ФОРМИ У КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ

2.1. Практика пошуку та фіксації доказів електронної форми у кримінальному процесі України

Практика пошуку, збирання, зберігання та використання доказів електронної форми поступово формується як окремий напрям кримінальної процесуальної діяльності, що вимагає спеціалізованих підходів. Водночас брак усталених алгоритмів, нормативна невизначеність щодо меж втручання у віртуальне середовище та складність фіксації мінливої цифрової інформації потребують глибокого аналізу практичних рішень на кожному з етапів роботи з досліджуваною формою доказів.

Питання фіксації доказів електронної форми досі не передбачає уніфікованого підходу в кримінальному процесі України. Це обумовлено як різновидом електронних носіїв інформації та інформаційних систем, так і різноманітними оперативними обставинами під час проведення слідчих (розшукових) дій. Ба більше, питання фіксації доказів електронної форми не обмежується інформацією, що міститься на фізичних носіях інформації. Не менш важливим та інформативним джерелом доказів для кримінального провадження є кіберпростір й інформаційні системи, доступ до фізичних систем яких обмежено. Усе це зумовлює потребу в універсальних стратегіях фіксації доказів електронної форми для застосування в кримінальному провадженні [119, с. 253–254].

Аналіз практики правозастосування дозволяє сформулювати комплекс алгоритмів пошуку та фіксації доказів електронної форми в кримінальному процесі України, що об'єднана за трьома функціонально-структурними категоріями², або

² Термін «функціонально-структурні категорії» передає саме цю двоєдину природу: структурний аспект визначає, у якому середовищі існують дані (фізичні носії, віртуальні простори, комбіновані системи); функціональний аспект відображає, яким чином учасник кримінального процесу взаємодіє з цим середовищем (вилучення, огляд, фіксація, копіювання).

ж три стратегії фіксації доказів електронної форми³ в кримінальному процесі України: 1) фізичне вилучення носія або інформаційної системи, до якої він входить; 2) огляд та копіювання інформації, що зберігається на електронному носії інформації; 3) огляд та фіксація інформації з відкритих джерел (кіберпростору⁴) (див. Додаток Г) [119, с. 254].

Пропоновані стратегії обумовлені такими аспектами: місцем знаходження інформації (кіберпростір або фізично визначені носії); юридичним статусом/станом інформації, інформаційної системи; технічним статусом/станом інформації, інформаційної системи; оперативною обстановкою під час проведення слідчих (розшукових) дій [119, с. 254].

Усі слідчі (розшукові) дії та НСРД в межах кримінального провадження так чи інакше реалізуються через одну з трьох зазначених стратегій. При цьому кожна з них передбачає специфічні вимоги як процесуального, так і технічного характеру, що потребують ґрунтового аналізу.

Пошук комп'ютерних систем, комп'ютерних пристроїв та електронних носіїв інформації у фізичному просторі є умовно «класичним» способом пошуку доказів електронної форми під час кримінального провадження. На відміну від традиційних речових доказів, сучасні електронні носії інформації можуть бути мініатюризованими, замаскованими або інтегрованими у предмети побуту, що суттєво ускладнює їх виявлення без спеціальних знань і технічних засобів. До стандартних носіїв належать персональні комп'ютери, ноутбуки, смартфони, планшети, зовнішні жорсткі диски, USB-флешки. Водночас у слідчій практиці дедалі частіше фіксується виявлення нетипових носіїв: GPS-трекерів, цифрових відеореєстраторів, годинників із вбудованою пам'яттю, мікрокарт пам'яті, схованих у меблях, побутових приладах або деталях одягу. Тактичні прийоми виявлення цифрових пристроїв мають адаптуватися до умов стрімкого розвитку ІТ та різноманіття форм-факторів.

³ Указані стратегії не розповсюджуються на фіксацію показань за допомогою технічних засобів, роботу з документами та висновками експертів, що є електронними документами в розумінні Закону України «Про електронні документи та електронний документообіг».

⁴ Термін застосовується як узагальнювальний.

За наявності доступу сторони обвинувачення під час проведення слідчих (розшукових) дій до носія інформації або інформаційної системи можливе застосування двох стратегій: або фізичне вилучення, або огляд та копіювання [119, с. 255].

Обшук — одна з важливих та високорезультативних слідчих (розшукових) дій, що проводиться з метою виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення, відшукування знаряддя кримінального правопорушення або майна, яке було здобуте у результаті його вчинення, а також встановлення місцеперебування розшукуваних осіб [46, с. 159–160]. Особливої ефективності дана слідча (розшукова) дія набуває в контексті можливості відшукування та вилучення комп'ютерів, ноутбуків, мобільних телефонів, що містять електронні носії інформації та є високоінформативними для досудового розслідування кримінального провадження. Водночас КПК України в ч. 2 ст. 168 КПК України суттєво обмежує сторону обвинувачення у можливості вилучення ЕІС, КС, МТСЗ.

Законодавець дозволяє тимчасове вилучення ЕІС, КС, МТСЗ, якщо вони безпосередньо не зазначені в ухвалі суду, в таких випадках: 1. надання комп'ютерної техніки разом з інформацією, що на ній міститься, є необхідною умовою проведення експертного дослідження; 2. комп'ютерна техніка отримана в результаті вчинення кримінального правопорушення; 3. комп'ютерна техніка є засобом або знаряддям вчинення кримінального правопорушення; 4. доступ до комп'ютерної техніки обмежується її власником, володільцем або утримувачем; 5. доступ до комп'ютерної техніки пов'язаний із подоланням системи логічного захисту. Таким чином, комп'ютерна техніка, носії інформації та телефони можуть бути вилучені слідчим під час обшуку, якщо вони безпосередньо зазначені в ухвалі суду та підпадають під один із п'яти приводів, зазначених у абз. 3 ч. 2 ст. 168 КПК України [161, с. 52-54].

Однак фізичне вилучення не є єдиним способом збирання доказів електронної форми. При виявленні під час слідчих (розшукових) дій ЕНІ збирання інформації, що міститься на них, як доказів може здійснюватися двома способами:

вилученням носія або інформаційної системи, до якого він входить, або копіюванням інформації, що зберігається на відповідному ЕНІ.

Вилучення як класичний спосіб збирання доказів у формі матеріальних об'єктів, до яких відносяться ЕНІ та інформаційні системи, попри всі очевидні переваги має низку недоліків. Зокрема, це стосується випадків неможливості вилучення або неефективності дослідження ЕНІ після вилучення у разі загрози зупинення критично важливих функцій бізнес-процесів або наявності шифрування тощо [125, с. 336–337].

Альтернативою є збирання інформації, що міститься в ЕНІ, як доказу в кримінальному провадженні шляхом виготовлення копії такої інформації. Відповідна процесуальна процедура з'явилась в КПК України лише у 2017 році й складається з таких компонентів: встановлення загальної заборони на тимчасове вилучення ЕІС, КС, МТСЗ із вичерпним переліком винятків (абз. 3 ч. 2 ст. 168 КПК України); передбачення права слідчого, прокурора здійснювати із залученням спеціаліста копіювання інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невіддільних частинах під час проведення огляду, обшуку (абз. 4 ч. 2 ст. 168 КПК України); визнання копії інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невіддільних частинах, виготовленої слідчим, прокурором із залученням спеціаліста як оригіналу документа (ч. 4 ст. 99 КПК України) [125, с. 337]. Логіку законодавця можемо прослідкувати за пояснювальною запискою до законопроекту, де метою таких змін вказано захист учасників кримінального провадження від необґрунтованого вилучення документів та комп'ютерної техніки та захист інтересів суб'єктів господарювання, які потерпають від фактичного блокування своєї діяльності внаслідок необґрунтованого вилучення комп'ютерної техніки та серверного обладнання в рамках кримінального провадження [219, с. 2–3].

Таким чином, в КПК України з'явився альтернативний спосіб збирання інформації, що має електронну форму, – збирання доказів електронної форми

шляхом копіювання інформації, для якого передбачено процесуальну форму, що можна представити як формулу: копія інформації × (слідчий або прокурор + спеціаліст) = оригінал документа [125, с. 337].

З огляду на положення ч. 4 ст. 99 КПК України вбачається, що виготовлена за наведеною процесуальною формулою копія електронної інформації є документом. Вказане є важливим для правильного розуміння правової природи копії електронної інформації як доказу в кримінальному провадженні. З урахуванням вимог абз. 3 ч. 2 ст. 168 КПК України та практики правозастосування слідчий, прокурор можуть зіткнутися з необхідністю виготовлення копії інформації в значній кількості випадків:

1. Під час проведення обшуку або огляду місця події копіювання інформації доцільно здійснювати: 1.1. при відсутності підстав для тимчасового вилучення майна; 1.2. при неможливості вилучення інформаційних систем через їх організаційну (структурну) складність або фізичну громіздкість; 1.3. при неможливості вилучення інформаційної системи через ризики припинення виробничого процесу; 1.4. при недоцільності вимкнення інформаційної системи через ризик втрати доступу до інформації (наприклад, за умови неможливості згодом успішно запустити розшифрування у разі вимкнення системи з активним шифруванням); 1.5. при копіюванні інформації з модулів оперативної пам'яті інформаційної системи; 1.6. при необхідності створення копії інформації для подання її разом із клопотанням до суду із метою накладення арешту на тимчасове вилучене майно - ЕНІ або інформаційну систему, на яких ця інформація виявлена; 1.7. при доцільності копіювання інформації для зменшення ризиків втрати інформації з первинного носія через його пошкодження або деградацію внаслідок впливу інших негативних факторів після вилучення;

2. Під час досудового розслідування також виникає необхідність виготовлення копії електронної інформації з ЕНІ, що вже знаходяться у володінні сторони обвинувачення (шляхом проведення огляду речей і документів) у таких випадках: 2.1. для подальшого детального вивчення, описання, друку конкретних документів, виявлених під час огляду; 2.2. для створення копії інформації ЕНІ з

метою зменшення ризику втрати інформації з первинного носія (виготовлення автономної копії-доказу з огляду на тактичну доцільність); 2.3. для видачі копії інформації особі, яка є володільцем цієї інформації та звернулася до слідчого з клопотанням про надання копії в порядку ч. 3 ст. 100 КПК України; 2.4. для долучення до кримінального провадження копії інформації з ЕНІ, замість оригінального ЕНІ, який за необхідності підлягає видачі особі, яка є володільцем носія та звернулася до слідчого з клопотанням про надання оригіналу цього ЕНІ в порядку ч. 3 ст. 100 КПК України; 2.5. з метою збереження інформації, що міститься на ЕНІ, у зв'язку із виконанням ухвали слідчого судді про повернення носія інформації власнику; 2.6. для створення копії інформації (як частини матеріалів досудового розслідування), щодо якої прокурором в порядку ч. 3 ст. 217 КПК України прийнято рішення про виділення матеріалів досудового розслідування в окреме провадження; 2.7. для створення копії інформації, отриманої за результатами проведення НСРД для використання в порядку ст. 257 КПК України; 2.8. для надання стороні захисту для ознайомлення та копіювання копії інформації замість оригіналу на етапі відкриття матеріалів кримінального провадження іншій стороні в порядку ст. 290 КПК України;

3. Крім того, відповідно до ч. 1 ст. 159 КПК України тимчасовий доступ до речей і документів здійснюється виключно шляхом зняття копії інформації, якщо доступ судом був наданий до ЕІС, КС, МТСЗ;

4. Виготовлення копії інформації в електронній формі як резервної копії оригінальних примірників технічних носіїв інформації зафіксованої процесуальної дії передбачено в ч. 3 ст. 107 КПК України. Резервні копії таких примірників дозволяється зберігати окремо від матеріалів кримінального провадження. Допустимість створених в такий спосіб резервних копій без участі спеціаліста визнається судом із врахуванням виключних підстав, передбачених п. 1 ч. 5 ст. 99 КПК України, коли оригінал документа втрачений або знищений не з вини сторони, яка його надає. Описані ситуації утворюють систему процесуальних сценаріїв, що передбачають необхідність виготовлення копії електронної інформації або ЕНІ під час кримінального провадження [125, с. 337].

Наведен система процесуальних сценаріїв у сукупності з розробленим алгоритмом прийняття рішень щодо вилучення ЕНІ під час обшуку, огляду [46, с. 159–165] спрямована на забезпечення слідчих, прокурорів методологією ефективної оцінки оперативної обстановки щодо прийняття рішень у частині поводження з ЕНІ. Якщо слідчим, прокурором за результатами аналізу оперативної обстановки під час проведення слідчих (розшукових) дій або з огляду на процесуальну необхідність прийнято рішення про здійснення копіювання інформації, що зберігається на ЕНІ, для забезпечення можливості використання такої інформації як доказу під час кримінального провадження необхідне дотримання двох аспектів: процесуального та технічного [125, с. 337-338].

Процесуальний аспект полягає в дотриманні слідчим, прокурором вимог ч. 4 ст. 99 КПК України щодо необхідності залучення спеціаліста, тобто дотримання наведеної нами попередньо формули. У даному аспекті варто зауважити, що формальне виконання вимоги КПК України щодо залучення спеціаліста не гарантує тотожності копії інформації оригіналу. Залучений стороною обвинувачення спеціаліст повинен володіти необхідними знаннями та навичками у сфері ІТ та бути здатним правильно реалізувати процес копіювання, що має включати верифікацію (перевірку) цілісності та справжності інформації з наданням відповідних гарантій. Варто звернути увагу на окремі випадки формального виконання слідчими вимог ч. 4 ст. 99 КПК України щодо залучення спеціаліста при копіюванні інформації, що має електронну форму, з одночасним недотриманням технічних аспектів щодо гарантування цілісності та справжності інформації, що може дискредитувати виготовлену копію [125, с. 338].

Таким чином, очевидно стає необхідність дотримання технічного аспекту процесу копіювання інформації, значення якого важко переоцінити.

Для забезпечення технічного аспекту процесу копіювання інформації доцільно застосовувати ДСТУ ISO/IEC 27037:2017. Стандарт розрізняє процеси виготовлення фізичної або порозрядної копії (образу) ЕНІ та копії окремого електронного файлу [125, с. 338].

ДСТУ ISO/IEC 27037:2017 детально визначають умови, за яких копіювання інформації для використання в юридичних процедурах може вважатися надійним і допустимим з технічного погляду. Загалом варто виділити дві вимоги: 1) недопустимість внесення змін до первинної інформації, що є об'єктом копіювання, до початку копіювання, під час та після його проведення. Одним з варіантів є підключення ЕНІ до комп'ютера спеціаліста чи слідчого здійснюється в режимі «тільки читання», наприклад, із використанням пристрою блокування запису; 2) верифікація (перевірка) копії інформації шляхом гешування первинної інформації, копії інформації та порівняння отриманих геш-значень. Це забезпечує можливість математично перевірити та підтвердити цілісність і справжність копії інформації, записаної на цільовий ЕНІ [83, с. 7].

Як слушно зауважують Яромір Вебер та Зденек Смутни (2015), стандарт ISO/IEC 27037:2012 «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence» (далі — ISO/IEC 27037:2012) у декількох місцях вказує на необхідність обрахування контрольних сум для перевірки цілісності даних, але при цьому недостатньо наголошено, що ці значення, отримані під час гешування, мають бути зафіксовані безпосередньо у протоколі процесуальної дії. Виконання цієї вимоги здатне забезпечити перевірку зібраних доказів на цілісність та справжність [526, с. 297]. Запровадження такої практики національними органами досудового розслідування матиме позитивний вплив.

Виготовлення копії інформації з дотриманням визначених у ДСТУ ISO/IEC 27037:2017 процедур та наведенням гарантій цілісності та справжності забезпечує можливість повторно перевірити й підтвердити цілісність та справжність копії інформації будь-яким технічним фахівцем у будь-який час, що створює переконливий та технічно досконалий для сторони обвинувачення доказ.

За умови дотримання стороною обвинувачення процесуальних та технічних аспектів при виготовленні копії інформації в електронній формі, утворюються унікальні умови гарантування цілісності та справжності даних копії, а відповідно — збирання допустимого доказу. Копія електронної інформації вже сьогодні є дієвим

інструментом доказування за умови дотримання процесуальних та технічних аспектів її виготовлення [125, с. 338].

Водночас з метою розширення практики використання копії електронної інформації як доказу в кримінальному провадженні, підвищення ефективності та забезпечення дотримання процесуальної процедури, пропонується вжити ряд адміністративних та організаційних заходів, серед яких: систематичне навчання та підвищення кваліфікації слідчих, прокурорів щодо роботи з доказами електронної форми; забезпечення органів досудового розслідування базовими технічними засобами (апаратними та програмними), призначеними для роботи з ЕНІ; створення в системі правоохоронних органів структурно та процесуально незалежних від органу досудового розслідування криміналістичних ІТ-лабораторій, що спеціалізуються на роботі з доказами електронної форми працівників яких може бути залучено як спеціалістів при проведенні слідчих (розшукових) дій для роботи з доказами електронної форми (за прикладом позитивного досвіду Національного антикорупційного бюро України (далі – НАБУ)); інформування суддів щодо технічних аспектів роботи з доказами електронної форми при проведенні спільних наукових та науково-практичних заходів, зокрема, із залученням Національної школи суддів України та міжнародних партнерів [125, с. 338].

Окрім того, необхідні системні зміни у підході до копії електронної інформації як доказу в кримінальному провадженні, що передбачають гарантування цілісності та справжності інформації не формальним залученням спеціаліста, а наданням гарантій незмінності первинної інформації з урахуванням вимог ДСТУ ISO/IEC 27037:2017. З огляду на це ч. 4 ст. 99 КПК України пропонуємо доповнити нормою щодо обов'язку спеціаліста підтвердити цілісність і справжність створеної копії інформації. Системний підхід до вдосконалення кримінальної процесуальної процедури та практики застосування в частині розширення можливостей використання копії інформації як доказу в кримінальному провадженні сприятиме ефективному збиранню доказів, забезпеченню прав як безпосередніх учасників кримінального провадження, так і

осіб, на яких може вплинути вилучення ЕНІ та інформаційних систем, мінімізації впливу кримінальних процесуальних процедур на бізнес-процеси [125, с. 339].

Разом з комп'ютерними даними під час проведення слідчих (розшукових) дій може бути виявлено не просто комп'ютерні дані чи носії інформації, а саме електронні документи в розумінні Закону України «Про електронні документи та електронний документообіг», що підписані електронним підписом. Порядок поводження з ними має свої особливості.

Під час досудового розслідування кримінальних правопорушень сторони провадження можуть вільно збирати електронні документи через їх копіювання, а під час судового розгляду – надавати суду їх примірники як докази, при цьому допустимість будь-якого й кожного примірника електронного документа визначається за правилами ч. 3 ст. 99 КПК України як надання оригіналу документа за умови підтвердження електронного підпису. Під час збирання доказів у стадії досудового розслідування сторони кримінального провадження можуть копіювати електронні документи (в розумінні Закону України «Про електронні документи та електронний документообіг» - прим. авт.) без залучення спеціаліста у сфері ІТ. Це стосується і випадку, коли стороні обвинувачення потрібно отримати електронний документ, який міститься на носії комп'ютерних даних у володінні інших осіб. За умови дотримання порядку проведення відповідної процесуальної дії (тимчасового доступу до речей і документів, обшуку, огляду тощо) слідчий, прокурор можуть скопіювати електронний документ самостійно [43, с. 75].

Обов'язок суду розглядати копії комп'ютерних даних як оригінал документа стосовно примірників електронних документів виникає у зв'язку з властивостями електронного документа і не потребує для досягнення такого правового наслідку (виникнення вказаного вище обов'язку суду) залучення спеціаліста з метою виконання умов порядку копіювання неспецифічних комп'ютерних даних, установленого ч. 4 ст. 99 КПК України.

Варто зазначити, що копіювання електронних документів слідчим, прокурором самостійно тактично допустимо лише у разі, коли є змога перед копіюванням електронного документа встановити його цілісність через перевірку

та підтвердження електронного підпису. Якщо ж за результатами перевірки електронного підпису такий підпис підтверджено, документ в електронній формі, до якого належить підпис, слід уважати електронним документом, цілісність і справжність якого доведено. У протилежному випадку для копіювання комп'ютерних даних слід залучити спеціаліста в галузі ІТ. Спеціаліст може бути залучений слідчим, прокурором до копіювання електронних документів також у разі потреби надання безпосередньої технічної допомоги, наприклад, через складність комп'ютерної системи, до якої здійснюється доступ, несправність носія комп'ютерних даних, необхідність перевірки електронних підписів на місці тощо [43, с. 75]. Зазначене свідчить про те, що під час роботи з електронними документами, зокрема тими, що містять КЕП, процесуальні дії можуть здійснюватися слідчим або прокурором самостійно, за умов наявності технічної можливості перевірки справжності підпису й цілісності документа. За відсутності таких умов або у разі ускладнень, пов'язаних з доступом, копіюванням чи технічними несправностями, доцільно залучати спеціаліста. Таким чином, електронні документи із підтвердженою автентичністю можуть бути включені до процесуального обігу як докази без спеціальних процедур криміналістичного аналізу, що значно спрощує їх використання під час кримінального провадження.

Разом із тим, з огляду на стрімку цифровізацію кримінального процесу, все частіше докази електронної форми виявляються не на фізичних носіях, а у віддалених віртуальних середовищах, зокрема хмарних платформах, акаунтах користувачів, сервісах онлайн-комунікацій та цифрових інфраструктурах, що не мають прив'язки до певного технічного пристрою. Така трансформація переміщує фокус слідчої діяльності у сферу віртуального простору, що функціонує за власною логікою та вимагає окремого методичного і правового підходу. У цьому контексті пошук, фіксація та збирання цифрових слідів у кіберсередовищі перетворюється на самостійний напрям розслідування, що потребує спеціалізованого інструментарію.

Пошук цифрової інформації у віртуальному просторі становить окремий напрям слідчої діяльності, що значно відрізняється від традиційних форм збору доказів у фізичному середовищі.

Відповідно до абз. 12 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», кіберпростір – середовище (віртуальний простір), яке дає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Кіберпростір складається із чотирьох рівнів: інфраструктурного, фізичного, синтаксичного й семантичного. Інфраструктурний рівень складається з радіоелектронної апаратури, ліній зв'язку, супутників, комп'ютерних мереж тощо. Фізичний рівень складається з усього того, що належить до ЕМС – електронів, фотонів, частот і т.п. – рівня, що дає життя інфраструктурному. Синтаксичний рівень складається з формату інформації й правил, що направляють і контролюють інформаційні системи, що утворюють кіберпростір. Семантичний рівень складається з інформації, корисної й зрозумілої користувачеві – людині й, по суті, є зв'язкою кібернетичного й когнітивного [500, с. 98]. При цьому фізичні елементи кіберпростору можуть бути територіально розміщені в різних містах чи навіть країнах, як і злочинці, що використовують можливості глобальної мережі. Варто звернути увагу, що це стосується не виключно кіберзлочинів, а також численних майнових, службових, корупційних та інших видів кримінальних правопорушень, докази який часто мають електронну форму і зберігаються у віртуальному середовищі.

Такий транскордонний (в територіальному аспекті) характер кіберпростору передбачає особливості правового регулювання проведення досудового розслідування, що вже реалізовані на міжнародному рівні [106, с. 116].

Базовим документом у цьому питанні є Конвенція про кіберзлочинність та Додатковий протокол до неї. Відповідно до ч. 2 ст. 19 Конвенції про кіберзлочинність, кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб у разі коли її компетентні

органи здійснюють обшук або подібний доступ до конкретної комп'ютерної системи або її частини відповідно до підпункту 1.а і мають підстави вважати, що дані, які розшуковуються, зберігаються в іншій комп'ютерній системі чи частині, яка знаходиться на її території, і до таких даних можна здійснити законний доступ з першої системи чи вони є доступними першій системі, такі компетентні органи мали право терміново поширити обшук або подібний доступ на іншу систему [148, с. 1]. Вважаємо, що дана норма передбачає можливість «розширення» обшуку з конкретної комп'ютерної системи або її частини на території певної держави (що здійснюється відповідно до встановленої процедури) на інші комп'ютерні системи чи її частини, що перебувають на території цієї ж держави. Вказане є логічним та не порушує територіального суверенітету інших держав, на території яких можуть перебувати фізичні елементи інформаційних систем, на яких зберігаються відомості [106, с. 117].

Законом України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам» від 15 березня 2022 р. № 2137-IX, частину 6 ст. 236 КПК України доповнено абзацом 2, відповідно до якого, якщо під час обшуку слідчий, прокурор виявив доступ чи можливість доступу до ЕІС, КС, МТСЗ, для виявлення яких не надано дозвіл на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що на них міститься, на місці проведення обшуку. Наведена норма мала б закріплювати в національному законодавстві можливість «розширеного обшуку», що передбачена в ч. 2 ст. 19 Конвенції про кіберзлочинність. Водночас з огляду на лінгвістичну конструкцію, що сформульована в абз. 2 ч. 6 ст. 236 КПК України, її зміст можна тлумачити по-різному [106, с. 117].

У вузькому значенні абз. 2 ч. 6 ст. 236 КПК України можна трактувати в розумінні ч. 2 ст. 19 Конвенції про кіберзлочинність, поширюючи можливість

проведення слідчої (розшукової) дії на комп'ютерні дані, що містяться в ЕІС, КС, МТСЗ, розташованих на території України. Однак відповідна норма не передбачає такої конкретизації. Фактично, національний законодавець передбачив дві умови: а) якщо є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні» та б) проведення такого пошуку на місці проведення «легального» обшуку, тобто за адресою, що визначена у відповідній ухвалі слідчого судді, суду. Таке тлумачення корелюється з нормами ч. 2 ст. 19 Конвенції про кіберзлочинність щодо територіального аспекту поширення проведення відповідної слідчої (розшукової) дії [106, с. 117–118].

У широкому розумінні абз. 2 ч. 6 ст. 236 КПК України можна трактувати поза контекстом ч. 2 ст. 19 Конвенції про кіберзлочинність, поширюючи можливість проведення слідчої (розшукової) дії (так званого «розширеного» обшуку) на комп'ютерні дані, що містяться в ЕІС, КС, МТСЗ, що розташовані будь-де у світі. Такий підхід можливий з огляду на відсутність «територіальних» обмежень на поширення проведення відповідної слідчої (розшукової) дії в даній нормі. Безумовно, застосування правоохоронцями такого підходу суттєво б спростило проведення відповідної слідчої (розшукової) дії та підвищило її ефективність. Але це, фактично, порушило б суверенітет держави, на території якої фізично знаходиться інфраструктура, на якій зберігається інформація, до якої отримано доступ [106, с. 118]. Окрім того, відповідно до ч. 4 ст. 9 КПК України у разі якщо норми цього Кодексу суперечать міжнародному договору, згода на обов'язковість якого надана ВР України, застосовуються положення відповідного міжнародного договору України.

З огляду на зазначене, норми абз. 2 ч. 6 ст. 236 КПК України необхідно трактувати у вузькому значенні, тобто у розумінні ч. 2 ст. 19 Конвенції про кіберзлочинність, що передбачає можливість розширення проведення слідчої (розшукової) дії на комп'ютерні дані, що містяться в ЕІС, КС, МТСЗ, розташованих виключно на території України.

Отже, всупереч спробам національного законодавця адаптувати положення міжнародного права щодо розширеного доступу до комп'ютерних систем, наявні формулювання вимагають уточнення та гармонізації з положеннями Конвенції про кіберзлочинність. Проблема транскордонного доступу до даних у межах досудового розслідування залишається відкритою, насамперед через обмеження, пов'язані з територіальним суверенітетом і складністю реалізації такого доступу без порушення міжнародних зобов'язань.

У такому контексті постає інша, не менш складна проблема: фіксація доказів електронної форми у ситуаціях, коли фізичний доступ до комп'ютерних систем чи носіїв інформації взагалі відсутній. Йдеться передусім про дані, що розміщені у хмарних середовищах чи цифрових платформах або таких, що транслюються у реальному часі без збереження на локальних носіях.

Відтак варто також звернути увагу на питання фіксації доказів електронної форми у разі відсутності доступу до фізичних носіїв, інформаційних систем, на яких фіксується або обробляється інформація: соціальні мережі; вебсайти або сервіси, сервери яких розташовані за межами території України; сервіси трансляції інформації без фіксації (поточкова інформація) та багато інших. Ключовою ознакою необхідності застосування цієї стратегії є відсутність фізичного доступу до інформації, інформаційної системи, що не дозволяє забезпечити копіювання інформації з фіксуванням контрольних сум даних на двох носіях інформації відповідно до стандартизованої методології [83] та вимог КПК України [119, с. 255].

Фіксація досліджуваних нами доказів у такій ситуації передбачає проведення огляду комп'ютерних даних у порядку ст. 237 КПК України з дотриманням вимог ч. 4 ст. 99 КПК України (для отримання інформацією статусу оригіналу документа). У такому випадку сторона обвинувачення може зафіксувати важливі відомості, що відображаються в презентаційній частині інформаційної чи програмної системи, доступної користувачу (frontend) щодо інформації, що знаходиться в публічному доступі. Для отримання відомостей, загальний доступ користувачів до яких обмежено, але які мають важливе значення для

кримінального провадження, можуть бути застосовані механізми Конвенції про кіберзлочинність та процедури міжнародного співробітництва під час кримінального провадження, визначені Розділом IX КПК України. Така стратегія передбачає:

1) огляд комп'ютерних даних в порядку ст. 237 КПК України з дотриманням вимог ч. 4 ст. 99 КПК України, фіксація та аналіз отриманої інформації, визначення місця перебування провайдера, адміністратора інформаційної системи, місця знаходження сервера тощо;

2) скерування до центрального уповноваженого органу відповідної іноземної держави, який відповідає за надсилання та відповідь на запити про взаємну допомогу, запиту про термінове збереження комп'ютерних даних, які зберігаються – в порядку ст. 16 Конвенції про кіберзлочинність. Запит має стосуватися відомостей, що не отримані під час огляду комп'ютерних даних, але які потенційно зберігаються у провайдера, адміністратора ресурсу, інших осіб чи організацій та які мають значення для кримінального провадження. Це можуть бути дані користувача при реєстрації в певному ресурсі, дані банківських карток, відомості про проведення фінансових операцій, дані про IP-адреси та MAC-адреси тощо. Важливо зауважити, що такий механізм варто застосовувати у разі загрози зникнення даних або незначного терміну їх зберігання. За результатами скерування даного запиту центральний уповноважений орган відповідної іноземної держави (при дотриманні вимог та процедур Конвенції про кіберзлочинність) забезпечить зберігання даних, про які вказано в запиті;

3) скерування до уповноваженого органу відповідної іноземної держави запиту про міжнародну правову допомогу в порядку ст. 551 КПК України для отримання даних, що збережені за результатами попередньо описаної процедури. За умови дотримання належної правової процедури відповідь компетентного органу іноземної держави міститиме запитувані стороною обвинувачення відомості, що збережено [119, с. 256].

За результатами описаних національних та міжнародних процедур (див. Додаток Є). стороною обвинувачення може бути отримано високоінформативний

доказ, котрий використовуватиметься як для пошуку інших доказів, так і для самостійного використання під час доказування. Безсумнівно, вибір правильної стратегії фіксації доказів електронної форми є запорукою отримання стороною обвинувачення інформативного та допустимого доказу, а також забезпечення виконання завдань кримінального провадження [119, с. 256-257].

Описана стратегія фіксації доказів електронної форми за відсутності фізичного доступу до інформаційних систем, ґрунтується на використанні наявного процесуального інструментарію та механізмів міжнародної правової допомоги під час кримінального провадження. Проте практика її реалізації у межах національного кримінального провадження демонструє фрагментарність і недостатню чутливість до технологічних особливостей цифрового середовища. Це зумовлює потребу у вдосконаленні чинних підходів та розвитку спеціалізованих процедур, здатних забезпечити достовірність і перевірюваність інформації, що здобувається в умовах віртуального простору.

На сьогодні огляд (ст. 237 КПК України) є основною та умовно «традиційною» слідчою дією для фіксації вмісту вебресурсів у кримінальному провадженні. Відповідна фіксація є ключовою для збереження доказової бази, виявленої в цифровому середовищі. Варто звернути увагу, що КПК України не містить окремої слідчої (розшукової) дії, що передбачала б огляд кіберпростору (що, можливо, варто виправити), як це передбачено для огляду трупа (ст. 238 КПК України), огляду трупа, пов'язаного з ексгумацією (ст. 238 КПК України). При цьому специфіка проведення огляду віртуального середовища межує з аналогічним рівнем специфіки, притаманної для згаданих різновидів. Так чи інакше, практика правозастосування підлаштовується під наявний в КПК України інструментарій. Однак огляд не є єдиною можливим варіантом фіксації віртуального середовища.

С. В. Самойлов (2025) справедливо зазначає, що слідчими діями, що можуть бути застосовані з цією метою, є огляд (ст. 237 КПК України) та слідчий експеримент (ст. 240 КПК України). З огляду на динамічну природу мережі Інтернет, існує необхідність точного відтворення та перевірки певних обставин, що зафіксовані в цифровій формі. Аналізуючи застосування слідчого експерименту та

огляду для фіксації вебресурсів, варто вказати на три важливі аспекти: динамічний характер вебресурсів; відтворення обставин доступу до вебресурсу; забезпечення об'єктивності та перевірюваності доказів. Основні параметри, що впливають на вміст відображених на екрані даних та які (додатково до визначених в КПК України) необхідно вказувати у протоколі слідчої (розшукової) дії: 1. Точні дата та час проведення слідчої дії – для фіксації стану вебресурсу на конкретний момент; 2. Операційна система та версія браузера – впливають на відображення вмісту вебресурсу; 3. Місцезнаходження (IP-адреса та параметри мережі) – може визначати регіональні налаштування контенту; 4. Обліковий запис користувача (якщо застосовується) – впливає на доступ до закритої інформації; 5. Наявність кешованих даних та налаштувань браузера – може впливати на завантажений контент; 6. Методи та засоби доступу до ресурсу – використання VPN, проксі-серверів, режиму інкогніто тощо; 7. Послідовність дій слідчого – точно відтворення кроків, що впливають на відображення сторінки; 8. Фіксація процесу – скриншоти, відеозапис, протокольний опис кожного етапу слідчої дії тощо. Порівняльний аналіз засвідчив, що застосування слідчого експерименту як слідчої дії у сфері фіксації вебресурсів є доцільним і обґрунтованим, стверджує С. В. Самойлов [244, с. 69].

Поряд з теоретичними аспектами варто також звернути увагу на практику правозастосування, що ілюструє доволі неоднозначні тенденції.

За результатами проведеного нами опитування суб'єктів кримінального провадження встановлено, що певну стандартизовану інструкцію/процедуру для фіксації джерела надходження доказу електронної форми (протоколювання та долучення до матеріалів кримінального провадження), використовують у своїй роботі 58% опитаних респондентів, не використовують 38%, іншу відповідь вказали 4% опитаних. При цьому відповіді окремих категорій респондентів на це питання суттєво відрізняються (див. Додаток В Рис. 4) [114, с. 80-81].

Варто зауважити, що відповіді суддів є очікуваними з огляду на характер їх повноважень. При цьому відповідні позиції щодо представників сторони обвинувачення об'єктивно потребують покращення. Це може бути реалізовано

шляхом розроблення та впровадження відомчих процедур фіксації доказів електронної форми, що наполегливо рекомендуватимуться до використання (СОП).

Під час проведеного нами опитування суб'єктів кримінального провадження у відповідь на питання, яка процедура фіксації джерела надходження доказу електронної форми, застосовується ними у роботі, респондентам пропонувалося надати короткі відповіді, які проаналізовано та згруповано в категорії (див. Додаток Б, Додаток В).

Отримані від респондентів відповіді свідчать про застосування таких процесуальних заходів як: проведення огляду з оформленням відповідного протоколу – 31%, складання протоколу слідчої дії (не деталізованого якого саме) – 21%; за правилами Протоколу Берклі – 11,4%; постанова про визнання речовим доказом – 3,5%; тимчасовий доступ до речей і документів — 33%; запит – 2,4%; НСРД – 2%; долучення рапортом – 1,8%; висновок експерта – 1,6%; журнал судового засідання – 1%; супровідний лист – 1%. При цьому такі відповіді як «запит», «долучення рапортом», «супровідний лист» надавали представники оперативних підрозділів та слідчі, а «журнал судового засідання» – виключно судді, «Протокол Берклі» – переважно прокурори. Вказане ілюструє кардинально різні підходи практиків до розуміння досліджуваного питання та свідчить про суттєву різницю в підходах різних органів [114, с. 81-82]. Також респонденти вказували про використання деяких технічних заходів та технологій, а саме: на носіях інформації – 4,7%; Електронний суд, АСДС – 4%; копіювання інформації – 3%; КЕП – 3%; фотофіксація – 3%; гешування – 3%; метадані – 2,76%; скриншот – 2,6%; архівування – 2,2%; відеозапис – 1,8%; дамп / програмні засоби – 1% (див. Додаток В Рис. 5). При цьому «Електронний суд, АСДС» – відповіді переважно адвокатів та деяких суддів; «гешування», «архівування», «копіювання», «метадані» – прокурорів та деяких суддів; «дамп» – виключно оперативних працівників кіберполіції [114, с. 82].

Також про методичні рекомендації ОГП окремо акцентували 1%, всі прокурори. Про практику вилучення оригіналів вказують 5,7% опитаних з різних

груп. Відсутня процедура фіксації джерела надходження електронного доказу у 14,3% респондентів, більшість з яких є адвокатами, а деякі – судьями. Примітно, що такі відповіді надали деякі слідчі та прокурори, що, на нашу думку, свідчить про потребу проведення додаткових навчальних заходів [114, с. 82]. Відповіді респондентів свідчать про брак у суб'єктів кримінального провадження цілісного бачення щодо практики пошуку, збирання та фіксації доказів електронної форми. Тому необхідно формувати таке бачення як шляхом розроблення й запровадження СОП, так і системного навчання всіх суб'єктів кримінального провадження.

Отже, аналіз пошуку, збирання та фіксації доказів електронної форми в кримінальному процесі України засвідчує наявність трьох базових стратегій: фізичне вилучення ЕНІ або систем, копіювання інформації, а також фіксація даних за відсутності доступу до фізичних носіїв. Кожна стратегія має окремі процесуальні умови застосування та технічні вимоги. Фізичне вилучення можливе лише за чітко визначеними підставами (ч. 2 ст. 168 КПК України), тоді як копіювання стало ефективною альтернативою, що вимагає залучення спеціаліста та дотримання технічних стандартів (зокрема, ДСТУ ISO/IEC 27037:2017). У разі відсутності фізичного доступу — зокрема при роботі з хмарними сервісами або вебресурсами — застосовуються механізми огляду комп'ютерних даних та, за потреби, міжнародного співробітництва.

Формування узгоджених підходів до фіксації доказів електронної форми потребує вдосконалення процесуального механізму, належного технічного оснащення та підвищення компетентності слідчих і прокурорів у сфері цифрової криміналістики. Водночас ключового значення набуває розроблення та впровадження національних підходів до механізмів підтвердження цілісності та справжності доказів електронної форми зокрема в межах доктрини *chain of custody* — безперервного та документованого контролю за рухом цифрового об'єкта з моменту його виявлення до використання в суді. Забезпечення процесуального та технічного контролю на всіх етапах обігу таких доказів є необхідною передумовою їх цілісності, а отже, і допустимості у кримінальному провадженні.

2.2. Механізми підтвердження цілісності та автентичності доказів електронної форми в кримінальному провадженні

У кримінальному процесі України провідне значення при фіксації ходу та результатів слідчих дій надається документуванню через призму протоколювання. Законодавчі вимоги до протоколу, як основного способу фіксації під час кримінального провадження, передбачені у статтях 104–106 КПК України й характеризуються доволі високим рівнем деталізації. У цьому контексті протокол виступає не лише носієм інформації, що відображає хід розслідування, а й інструментом підтвердження законності дій, що здійснюються уповноваженими суб'єктами кримінального провадження.

Під час роботи з доказами електронної форми відповідні вимоги до протоколювання набувають особливої ваги. Протокол має забезпечувати якість доказу електронної форми; тобто має бути гарантована можливість довіри до зафіксованого цифрового об'єкта як джерела достовірної інформації, сформованої та закріпленої з дотриманням вимог кримінального процесуального закону.

З метою забезпечення належної ідентифікації доказів електронної форми під час кримінального провадження, у березні 2022 р. внесено деякі зміни до КПК України. Так, п. 3 ч. 3 ст. 104 КПК України доповнено абзацом, відповідно до якого прикінцева частина протоколу повинна містити «виготовлені дублікати документів, а також копії інформації, у тому числі комп'ютерних даних, та способів їх ідентифікації» [224, с. 1]. Разом зі змінами до ст. 99 КПК України щодо введення терміну «комп'ютерні дані» доповнення ч. 2 ст. 237 КПК України абзацом другим щодо врегулювання питання огляду комп'ютерних даних та низкою інших нововведень, законодавець належно врегулював питання фіксації доказів електронної форми та виявлених на носії інформації, який не може бути вилучений [118, с. 71]. Однак важливо зауважити саме на положеннях п. 3 ч. 3 ст. 104 КПК України щодо відображення в протоколі відомостей про «копії інформації, у тому числі комп'ютерних даних, та способів їх ідентифікації», що є надзвичайно актуальним та безпосередньо пов'язане з допустимістю такого доказу.

Термін «ідентифікація» походить від пізньолат. *identifico* — ототожнюю. Теорія ідентифікації вивчає технічні засоби, методи та прийоми встановлення тотожності об'єктів, що мають значення для розслідування злочину [152, с. 18]. Отож, відображення в протоколі способу ідентифікації комп'ютерних даних має забезпечити можливість встановлення тотожності комп'ютерних даних, що досліджуються на різних стадіях (етапах) кримінального провадження, з первинними комп'ютерними даними, що виявлені та/або зафіксовані під час слідчої (розшукової) дії та за результатами яких складено такий протокол [118, с. 72], тобто його цілісності та автентичності [94, с. 209].

Щодо умовно «традиційних» доказів як, наприклад, різні предмети або об'єкти, способом ідентифікації є опис в протоколі, фотографування, упакування із засвідченням підписами учасників слідчої (розшукової) дії тощо. Щодо доказів електронної форми та, зокрема, комп'ютерних даних вказане також актуально, однак з огляду на їх цифрову природу внесення змін до них не спричиняє розбірливості для людського ока візуальні ознаки. Відтак способи ідентифікації комп'ютерних даних для завдань кримінального провадження мають забезпечувати підтвердження їх цілісності та автентичності з набагато вищим ступенем вірогідності, ніж це можуть зробити традиційні способи ідентифікації [118, с. 72].

На основі практики правозастосування можемо окреслити цілу низку способів ідентифікації, що їх можна застосовувати під час кримінального провадження щодо доказів електронної форми:

1. Упакування та фізичне маркування носія. Найбільш базовим елементом ідентифікації носія інформації, що водночас відіграє важливу роль у забезпеченні цілісності даних, є його належне упакування та документальне оформлення. Вилучений носій підлягає упакуванню в індивідуальну тару (конверт, пакет, ємність), яка маркується з обов'язковим зазначенням дати, часу, місця вилучення, підписів осіб, що проводили слідчу дію, та застосуванням засобів захисту від несанкціонованого доступу (опечатування, пломбування, накладення індикаторних етикеток тощо). Таке оформлення слугує первинною гарантією недоторканності об'єкта та збереження його доказової цінності;

2. Загальні ідентифікаційні характеристики носія інформації. У цьому аспекті здійснюється фіксація фізичних та технічних параметрів носія, що дозволяють його розпізнати. Йдеться про зазначення типу цифрового пристрою (USB-накопичувач, жорсткий магнітний диск, SSD, карта пам'яті, оптичний диск тощо), загального обсягу пам'яті, кольору, форми, наявності фізичних пошкоджень, сторонніх написів, етикеток, наклейок, логотипів виробника тощо;

3. Унікальні ідентифікатори апаратного рівня носія інформації. До цього способу ідентифікації належать серійні номери, MAC-адреси, унікальні ідентифікатори пристрою (Device ID), які присвоюються виробником та зберігаються у внутрішній пам'яті пристрою незалежно від вмісту користувача. Наприклад, серійний номер жорсткого диска або SSD дозволяє однозначно ідентифікувати пристрій навіть після форматування або часткового знищення файлів. Використання таких апаратних ознак значно підвищує достовірність встановлення тотожності об'єкта дослідження у разі наявності кількох подібних носіїв;

4. Характеристики вмісту носія інформації (даних). Цей спосіб ідентифікації пов'язаний з документуванням вмісту носія: структури каталогів, назв файлів, їхніх розмірів, типів, розширень, а також наявності системних або прихованих файлів. Під час слідчої або процесуальної дії може бути складено перелік усіх виявлених даних, що може супроводжуватися коротким описом їхнього змісту (наприклад, «текстовий документ із назвою договору», «відеофайл, що містить запис переговорів» тощо);

5. Метадані та системна інформація. До цієї категорії належать метадані, тобто службова інформація, що автоматично генерується під час створення, редагування або збереження файлів. Вона охоплює дату й час створення, останнього редагування та відкриття файлу, відомості про користувача або ПЗ, яким файл був створений, а також журнал подій операційної системи, якщо він збережений. Особливу цінність становлять метадані, що не відображаються у звичайному користувацькому інтерфейсі, але можуть бути виявлені шляхом застосування спеціалізованих інструментів цифрової криміналістики;

6. Гешування та геш-сума. Найвищий рівень точності верифікації доказів електронної форми забезпечується застосуванням гешування — математичної операції, яка на основі вмісту файлу або цілого носія формує унікальний цифровий ідентифікатор (геш-значення). Найпоширенішими у правозастосовній практиці є алгоритми MD5, SHA-1, SHA-256, які використовуються для створення контрольних сум. Будь-яка, навіть незначна зміна вмісту файлу змінює його геш-суму, що дозволяє чітко встановити факт втручання в цифрову інформацію. У разі збігу геш-сум двох файлів цифрова криміналістика вказує, що вони є двома екземплярами одного і того ж файлу [94, с. 210-211].

Як бачимо, п. 3 ч. 3 ст. 104 КПК України вимагає відображення в протоколі способу ідентифікації комп'ютерних даних, однак ніде в КПК України чи відомчих НПА не вказано вимог або рекомендацій щодо цього. Отож вибір способу ідентифікації доказу електронної форми, корелюється з рівнем технічної освіченості суб'єктів, які беруть участь у певній слідчій (розшуковій) чи процесуальній дії, а також обумовлений регіональною практикою правозастосування і навіть наявними «шаблонами» протоколів слідчих дій, що містять певні «графи» для заповнення.

Зауважимо, що правозастосовна практика ілюструє доволі неоднозначні тенденції. Як результат проведеного нами опитування суб'єктів кримінального провадження встановлено, що певну стандартизовану інструкцію/процедуру для перевірки цілісності (вірогідності) доказу електронної форми, використовують у своїй роботі 38% опитаних респондентів, не використовують 59%, іншу відповідь указали 3% опитаних. При цьому відповіді окремих категорій респондентів на це питання так само суттєво відрізняються (див. Додаток В Рис. 6) [114, с. 80-81].

Тривожною є тенденція щодо використання відповідних процедур лише 43% слідчих / детективів та 36% прокурорів. При цьому серед слідчих та прокурорів, що використовують процедури для перевірки цілісності електронного доказу, понад 70% використовують докази досліджуваної категорії «часто» або «дуже часто», що свідчить про зв'язок між практикою правозастосування та технічною освіченістю правників. Однак така ситуація ставить під загрозу порушення цілісності або

потенційної неспроможності її підтвердити щодо значної частини зібраних під час досудового розслідування доказів електронної форми.

На питання «Яку процедуру перевірки цілісності (достовірності) доказів електронної форми Ви застосовуєте у своїй роботі?» респондентам пропонувалося дати короткі відповіді, які проаналізовано (у деяких випадках розділено на частини), узагальнено та згруповано в такі категорії: «Гешування / контрольні суми» – 17%; «КЕП» – 14%; «Протокол огляду / Протокол Берклі» – 10%; «Відповідно до вимог КПК України» – 9%; «Експертиза» – 6%; «Візуальний перегляд / за допомогою ПЗ» – 6%; «За результатами дослідження в судових засіданнях та з урахуванням позицій сторін кримінального провадження» – 3%; «Огляд оригіналу» – 2%; «OSINT» – 2% (див. Додаток Б, Додаток В Рис. 7). При цьому 36,4% опитаних цілісність доказів не перевіряють; зокрема (за часткою від загальної кількості опитаних респондентів відповідної категорії) 14% адвокатів, 35% оперативних працівників, 39% прокурорів, 29% слідчих / детективів та 21% суддів. Тобто стороною обвинувачення перевірка цілісності доказів електронної форми не завжди здійснюється, однак і адвокатами майже не ініціюється, що є дуже цікавою тенденцією. Тому можемо припустити, що поточний стан використання стандартизованих інструкцій/процедур для перевірки цілісності (достовірності) доказів електронної форми та проведення відповідних перевірок обумовлений відсутністю потреби, спричиненою позицією сторони захисту.

За результатами відповідей на питання «Як у Вашій практиці відбувається зберігання доказів та їх долучення до матеріалів кримінального провадження?» встановлено, що зберігання доказів після долучення (на фізичних носіях (ПК або фізичні носії інформації (флешки, диски, жорсткі диски тощо), на хмарних сервісах) присутнє в практиці 82% респондентів; копіювання або вилучення доказів – 71%. Частина респондентів вказали власні відповіді, зокрема практикується систематизація доказів для подальшого використання у 16% опитаних, додавання доказів до внутрішніх систем відомства – 5%, відсутня така практика у 2% опитаних (серед яких переважно судді та адвокати) (див. Додаток Б, Додаток В Рис. 8).

Аналізуючи норми п. 3 ч. 3 ст. 104 КПК України щодо способів ідентифікації, застосовуваних під час кримінального провадження щодо доказів електронної форми необхідно звернутися до ДСТУ ISO/IEC 27037:2017, що надає настанови для специфічної діяльності з оброблення доказів електронної форми⁵, а саме: ідентифікації, збирання, здобуття та збереження доказів електронної форми що можуть мати доказове значення. Цей стандарт надає настанови для спеціалістів стосовно звичайних випадків, які трапляються в процесі оброблення цифрових доказів, та допомагає організаціям в їхніх дисциплінарних процедурах та забезпеченні обміну потенційними доказами електронної форми між юрисдикціями [83, с. 1]. З огляду на відсутність регулювання в КПК України та підзаконних НПА відповідних технічних процедур, вбачається, що норми даного стандарту в технічному аспекті застосовні щодо роботи з доказами електронної форми під час кримінального провадження [118, с. 72–73]. Аналогічну думку висловлює А.М. Гаркуша [44, с. 44-45].

Згідно з п. 3.12 ДСТУ ISO/IEC 27037:2017 ідентифікація (identification) — це процес, який охоплює пошук, розпізнавання та документування потенційних доказів електронної форми. Відповідно до п. 5.4.2 ДСТУ ISO/IEC 27037:2017 процес ідентифікації вміщує пошук, розпізнавання та документування потенційного доказу електронної форми [83, с. 6]. Ці значення терміну «ідентифікація» варто диференціювати. У розумінні ДСТУ ISO/IEC 27037:2017 процедура ідентифікації доказів електронної форми асоціюється радше з пошуком та передує збиранню доказів, тоді як для завдань п. 3 ч. 3 ст. 104 КПК України способи ідентифікації комп'ютерних даних передбачають (з огляду на загальну логіку відповідного пункту цієї норми) спосіб підтвердження цілісності та автентичності комп'ютерних даних [118, с. 73].

Категорії «цілісність» (або ж незмінність, гарантія того, що цифровий об'єкт з моменту його виявлення або створення не зазнавав змін у змісті чи структурі, а

⁵ У ДСТУ ISO/IEC 27037:2017 переклад з англ. «digital evidence» — «цифровий доказ», однак для виконання завдань цього дослідження використовується термін «доказ електронної форми», щоб забезпечити послідовність застосування термінології в тексті дослідження.

отже, зберігає свій первинний стан) та «автентичність» (здатність підтвердити, що дані походять саме з того джерела, яке вказується, без фальсифікацій чи підміни) наразі не відображені⁶ в КПК України. Водночас ДСТУ ISO/IEC 27037:2017 установлює, що такі процеси, як ідентифікація, збирання, здобуття та збереження, потрібні під час слідства для підтримання цілісності доказів електронної форми – прийнятна методологія їх отримання, яка буде забезпечувати їхню допустимість у законодавчих та дисциплінарних судових процесах, а також інших потрібних інстанціях. Тобто цілісність доказів електронної форми виступає умовою їх допустимості⁷, що є логічним з огляду на процесуальну спрямованість відповідної категорії в кримінальному процесі України [94, с. 212].

У контексті попередньо розглянутих нами способів ідентифікації, що їх може бути застосовано під час кримінального провадження щодо доказів електронної форми ДСТУ ISO/IEC 27037:2017 визначає вимоги документувати всі унікальні ідентифікатори цифрових пристроїв та приєднаних частин, таких як серійні номери та унікальне маркування (п. 6.6; п. 7.1.1.1.), характеристики даних (системно описано процедуру фіксації в багатьох пунктах), виготовлення криміналістичної (побітової) копії (п. 5.4.4.) та необхідність обчислення та документування геш-

⁶ Єдиним винятком є вимога ч. 4 ст. 263 КПК України, що зобов'язує керівників та працівників операторів електронних комунікацій сприяти виконанню дій із зняття інформації з електронних комунікаційних мереж, вживати необхідних заходів щодо нерозголошення факту проведення таких дій та отриманої інформації, зберігати її в незмінному вигляді. Однак така вимога спрямована на інших учасників кримінального провадження, а не представників суб'єктів, що переважно забезпечують відшукання та збирання доказів. До того ж норма стосується лише одного виду НСРД. Тому цим винятком можна загалом знехтувати в світлі системної неврегульованості в КПК України питання забезпечення цілісності доказів електронної форми.

⁷ Допустимість доказу в кримінальному процесі України є однією з ключових категорій інституту доказування та тісно пов'язана із суворим дотриманням процесуальних приписів на всіх етапах його існування. Так, відповідно до ч. 1 ст. 86 КПК України, доказ визнається допустимим, якщо він отриманий у порядку, встановленому цим Кодексом. Згідно з ч. 1 ст. 87 КПК України недопустимими є докази, отримані внаслідок істотного порушення прав та свобод людини, гарантованих Конституцією та законами України, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, а також будь-які інші докази, здобуті завдяки інформації, отриманій внаслідок істотного порушення прав та свобод людини.

Фактично допустимість доказу є процесуальним визнанням його придатності до використання у доказуванні, що передбачає дотримання вимог законності під час його пошуку*, фіксації** та використання. Йдеться, зокрема, про дотримання прав і свобод людини, правомірність проведення слідчих (розшукових) дій тощо. У своїй сукупності ці елементи спрямовані на забезпечення прав і свобод учасників кримінального провадження, створення процесуальних гарантій, що дозволяють вважати отриману інформацію такою, що заслуговує на довіру з боку суду.

значень (п. 7.1.3.1.2). Тобто ДСТУ ISO/IEC 27037:2017 не визначає якийсь один спосіб ідентифікації для доказів електронної форми а пропонує комплексну методологію щодо роботи з ними. Власне, у вступі до ISO/IEC 27037:2012, на основі якого розроблено (фактично, просто перекладено без адаптації) ДСТУ ISO/IEC 27037:2017, зазначається, що завдяки недовговічності доказів електронної форми потрібно мати прийнятну методологію для гарантування цілісності та автентичності потенційних доказів електронної форми не вимагає обов'язкового використання виняткових інструментів або методів. Ключовим компонентом, який забезпечує довіру в розслідуваннях, є методологія, яку застосовують протягом цього процесу, та особи, що мають кваліфікацію для виконання завдань, визначених цією методологією [83, с. V].

Усвідомлення такої відмінності змінює парадигму нашого дослідження в цьому підрозділі. Особливістю вітчизняної моделі кримінального процесу є її належність до романо-германської правової системи, в межах якої превалює формалізований підхід, в тому числі до процесу доказування. Це зумовлює суворе регулювання як порядку збирання доказів, так і вимог до документів, що їх фіксують. Такий підхід забезпечує високий рівень юридичної визначеності. Натомість в англо-американській правовій традиції у досліджуваних нами сфері превалює інша концептуальна модель – *chain of custody*, що є інструментом підтвердження автентичності та цілісності доказу в кримінальному провадженні. В її основі лежить забезпечення прозорості та простежуваності процесу поводження з доказом на всіх етапах його обігу – від моменту виявлення до представлення в суді. Такий підхід передбачає документальну фіксацію кожної зміни місця знаходження, форми існування чи володільця доказу, що дозволяє виключити сумніви у підробці, фальсифікації або втручанні [94, с. 213]. І саме цей підхід прослідковується в ДСТУ ISO/IEC 27037:2017. Пункт 6.1 ДСТУ ISO/IEC 27037:2017 передбачає вимоги щодо забезпечення хронологічного документування⁸. Вказаний пункт визначає, що у будь-яких дослідженнях перший

⁸ Оригінальний варіант назви цього пункту англійською мовою в ISO/IEC 27037:2012, IDT «Chain of custody».

відповідальний за доказ електронної форми або ж Digital Evidence First Responder (далі – DEFR) повинен мати змогу звітувати про всі здобуті дані та прилади в той час, коли вони знаходяться під захистом DEFR. Запис хронологічного документування (переклад в ДСТУ з англ. chain of custody – прим. авт.) є документом, який показує хронологію переміщень та оброблення потенційних доказів електронної форми. Вона має охоплювати час від процесу збирання або здобуття. Зазвичай, її супроводжує простежування історії елемента від часу, коли його було ідентифіковано, зібрано або здобуто командою дослідників до поточного статусу та місця знаходження. Запис хронологічного документування є документом чи набором пов’язаних документів, які деталізують хронологічне документування, та записи, хто відповідав за оброблення потенційних доказів електронної форми або у вигляді доказів електронної форми або в іншому форматі (як паперові нотатки). Метою підтримання записів хронологічного документування є змога ідентифікації доступу та переміщення потенційних доказів електронної форми у будь-якій точці часу. Самі записи хронологічного документування можуть містити більше ніж один документ, наприклад, для потенційних доказів електронної форми має бути сучасний документ, у якому записано здобуття цифрових даних на конкретному пристрої, переміщення цього пристрою та документація, яка містить послідовні виписки або копії потенційних доказів електронної форми для аналізування та інших цілей. Записи хронологічного документування мають містити таку інформацію, щонайменше: унікальний ідентифікатор доказу; хто мав доступ до доказу та час і місце, де це зроблено; хто перевіряв доказ під час введення в та виведення з обладнання збереження доказу та коли це було зроблено; чому доказ було перевірено (в якому випадку та з якою метою) та відповідний дозвіл, якщо його було надано; будь-які невідворотні зміни в потенційних цифрових доказах, а також ім’я особи, відповідальної за це та юрисдикцію для внесення цих змін.

Хронологічне документування має бути підтримуване протягом усього часу життя доказів та зберігатися впродовж визначеного періоду часу після завершення часу життя доказів — цей період часу може бути встановлено відповідно до

локального законодавства збирання та застосування доказів. Його має бути встановлено від моменту, коли цифрові прилади та/або потенційні докази електронної форми здобуто, й не повинен змінюватися [83, с. 1–31].

Отже, постає об'єктивна потреба у комплексному аналізі концепції *chain of custody* як усталеної міжнародної практики при роботі з доказами електронної форми. Такий аналіз дозволить окреслити напрями імплементації найкращих міжнародних стандартів у вітчизняну практику та розробити науково обґрунтовану модель роботи з доказами електронної форми.

М. І. Пашковський (2024) вказує, що ланцюг зберігання (англ. – *chain of custody*) є методом забезпечення хронологічної нерозривності законного володіння (збирання, збереження, подальшого поводження, зокрема переміщення та розпорядження) уповноваженими особами доказами у кримінальному провадженні з моменту їх (як потенційних доказів) виявлення або отримання до їх (доказів) поточного статусу і місцеперебування. З іншого боку, протокол ланцюга зберігання є документом або серією пов'язаних документів, які детально фіксується ланцюг зберігання [186, с. 159].

Ланцюг зберігання (*chain of custody*) є необхідним для підтвердження того, що докази, представлені в суді, є справжніми й не підробленими. Процес *chain of custody* забезпечує це шляхом ретельної фіксації (документування) кожного етапу руху доказів протягом усього життєвого циклу справи. Документація ланцюга зберігання повинна містити наступну інформацію:

- Що? (What?) Що є доказом?
- Як? (How?) Як його було зібрано та збережено?
- Хто? (Who?) Хто взяв його у володіння?
- Коли? (When?) Коли його було зібрано, передано або оброблено?
- Куди? (Where?) Куди перемістився доказ?
- Чому? (Why?) Чому доказ було передано? [462, с. 13]. Науковці ще визначають описаний принцип як п'ять "W" і один "H" [363; 364].

Chain of custody має містити детальний опис оброблення доказів, включаючи відомості про персональні дані, місцезнаходження та дії осіб, які брали участь у

їхньому дослідженні та аналізі. Ця вичерпна документація забезпечує цілісність доказів та підвищує прозорість і підзвітність протягом усього криміналістичного процесу. У судових процесах chain of custody має вирішальне значення для підтвердження версії слідства [462, с. 13].

З моменту збору доказів до моменту їх представлення в суді завжди має бути зрозуміло, де знаходилися докази, хто їх зберігав і що з ними сталося, якщо таке сталося. Це називається ланцюгом зберігання (chain of custody). Сенсом існування ланцюга зберігання (chain of custody) є підтвердження факту того, що докази дійсно пов'язані зі злочином, а не є сфабрикованими, тобто підтвердження їх допустимості. Ланцюг зберігання (chain of custody) вимагає, щоб з моменту збору доказів кожна їх передача від однієї особи до іншої була задокументована і щоб можна було довести, що ніхто інший не мав доступу до цих доказів. Таким чином, якщо під час судового розгляду допустимість доказу будуть оскаржувати шляхом поставлення під сумнів ланцюга зберігання доказів, можна буде довести, що як дані, так і носій інформації є справжніми. Однак якщо є розбіжності й це не може бути доведено, то ланцюг зберігання порушується й може бути подано клопотання про визнання доказів недопустимими [94, с. 215].

Chain of custody тісно пов'язаний з життєвим циклом доказу. Не існує чіткого визначення життєвого циклу доказів електронної форми але можна використовувати визначення цифрового файлу та цифрового архівування. Згідно з Gail M. Hodge (2000) [422] життєвий цикл інформації складають декілька фаз: 1. Створення (Creation); 2. Придбання та збирання (Acquisition and collection); 3. Ідентифікація та каталогізація (Identification and cataloguing); 4. Зберігання (Storage); 5. Збереження (Preservation); 6. Доступ (Access) [365, с. 127].

Nath S., Summers K., Baek J. and Ahn G.J. (2024) життєвий цикл доказів електронної форми від ідентифікації до представлення в суді, поділяють на шість етапів: 1. Ідентифікація (Identification); 2. Збирання (Collection); 3. Збереження (Preservation); 4. Дослідження (Examination); 5. Аналіз (Analysis); 6. Представлення (Presentation) [462, с. 12].

Cosic J. and Cosic Z. (2012) зазначають, що життєвий цикл доказів електронної форми має певну схожість. Перша фаза життєвого циклу такого доказу не є створенням, оскільки в процесі цифрового розслідування ми вже маємо цифровий файл, який був створений раніше. Цей файл стане доказом у майбутньому. Перша фаза їх життєвого циклу – це ідентифікація та збір. На цьому етапі фахівці з цифрової криміналістики повинні провести пошук у величезній кількості матеріалів, щоб знайти щось цікаве (принцип айсберга). Ця фаза дуже складна і має більше впливу, що може порушити ланцюг зберігання доказів. Наступним етапом життєвого циклу є експертиза. На цьому етапі з доказами електронної форми можуть контактувати судові слідчі та свідки-експерти. Етап дослідження передбачає ідентифікацію потенційних доказів та відокремлення інших великих обсягів цифрових файлів. Процес зберігання та транспортування – це етапи, які завжди відбуваються в цьому колі. Весь ланцюг зберігання доказів електронної форми повинен бути замкнутим. Черговим етапом життєвого циклу доказів електронної форми є підготовка звіту чи публікації. Це не завершальна фаза. На цьому етапі докази представляються стороною захисту чи обвинувачення, і з досліджуваними доказами можуть контактувати експерти, свідки-експерти, захист і обвинувачення. Будуть представлені результати судових розслідувань. Нарешті, є етап закриття справи, на якому докази електронної форми можуть бути збережені та заархівовані. Отже, що життєвий цикл доказів електронної форми починається з ідентифікації та збору, продовжується звітом про експертизу та публікацією і закінчується зберіганням та архівацією [365, с. 128].

Життєвий цикл доказів електронної форми є дуже складним, і на кожному етапі існує більше впливів, які можуть порушити ланцюг зберігання [365, с. 127]. Якщо докази електронної форми використовуються в міжнародному розслідуванні, цей життєвий цикл є більш складним, і його важко зберегти.

Робота з доказами електронної форми передбачає наявність складної мережі зацікавлених сторін і технологій, що лежать в основі систематичних і науково обґрунтованих розслідувань, пов'язаних з такими доказами [462, с. 12].

Cosic J. and Cosic Z. (2012) акцентують увагу на переліку осіб, які можуть взаємодіяти з доказами електронної форми: служби швидкого реагування; слідчі; спеціалісти та експерти; працівники правоохоронних органів; працівники поліції (інспектори карного розшуку); потерпілий; підозрюваний; перехожий. Кожен з них може впливати на докази в конкретній ситуації, а тому дуже важливо знати відповідь на питання «Хто контактує з доказами?» [365, с. 127].

За даними Міжнародної організації з комп'ютерних доказів (IOCE) [427, с. 1], коли особі необхідно отримати доступ до оригінальних доказів електронної форми ця особа повинна пройти відповідну підготовку. У багатьох випадках це неможливо, оскільки криміналістика є дуже складною наукою і вимагає високого рівня кваліфікації для роботи з доказами [365, с. 127].

Chain of custody в частині доказів електронної форми у західній науковій традиції є предметом дослідження упродовж не одного десятиліття. Nath S., Summers K., Baek J. and Ahn G.J. (2024) зазначають, що нещодавні дослідження та настанови окреслили безліч важливих вимог до chain of custody для доказів електронної форми. Попри різні підходи, всі вони мають спільні цілі та включають такі вимоги: 1. Цифровий chain of custody повинен бути всеосяжним, що дає змогу документувати різноманітні судово-експертні дії на різних етапах процесу розслідування. 2. Цифровий chain of custody має бути повним, гарантуючи, що кожна судово-експертна діяльність у процесі розслідування задокументована з безперервною безперервністю. 3. Зберігання та збереження доказів електронної форми повинно підтримувати високий рівень безпеки, підтримуючи всі три аспекти безпеки - конфіденційність, цілісність та доступність. 4. Після внесення та затвердження записів до chain of custody вони повинні залишатися незмінними та непорушними. 5. Усі зацікавлені сторони, які взаємодіють з доказами та chain of custody, повинні бути неспростовно автентифіковані для забезпечення неможливості відмови від них, надаючи неспростовні докази їхньої особи. 6. Цифровий chain of custody повинен бути перевірений усіма зацікавленими сторонами, залученими до судово-експертної екосистеми. 7. Цифровий chain of custody повинен забезпечувати дотримання

заходів контролю доступу, враховуючи різні фактори, зокрема роль зацікавленої сторони в розслідуванні та характер доказів. 8. Моделі chain of custody мають бути придатними для впровадження в реальному світі та приносити відчутні вигоди. 9. Програмна платформа (framework) повинна мати інтуїтивно зрозумілий і зручний дизайн з прийнятною складністю і здатністю до навчання, щоб врахувати різноманітний досвід зацікавлених сторін у судово-експертній діяльності. 10. Chain of custody повинен збалансувати потреби в обчислювальних (пропускна здатність, сховище, потужність тощо) і необчислювальних (фізичний простір, людські ресурси тощо) ресурсах, враховуючи бюджетні обмеження і наявність ресурсів. 11. Програмна платформа (framework) повинна враховувати як прямі витрати, так і потенційні зобов'язання, особливо при використанні послуг третіх сторін для зберігання доказів та/або розгортання системи [462, с. 13–14].

Поряд з загальними вимогами до chain of custody в частині доказів електронної форми практика їх реалізації характеризується різним ступенем інтеграції сучасних технологій в процес документування та різновидом останніх. Nath S., Summers K., Baek J. and Ahn G.J. (2024) виділяють три різновиди chain of custody:

1. Традиційний паперовий chain of custody - передбачає використання традиційних паперових форм та ґрунтується на детальному документуванні для фіксації важливої інформації на етапах збору, дослідження та аналізу доказів. Попри свою простоту, паперовий підхід chain of custody має кілька переваг. Він забезпечує прозорість, пропонуючи чіткий і простежуваний запис взаємодії доказів, що є надзвичайно важливим для судових проваджень. Цей метод гарантує підзвітність, обмежуючи доступ і вимагаючи підписів уповноваженого персоналу, тим самим посилюючи безпеку та відповідальність. Крім того, фізичні форми підлягають суворому контролю фізичного доступу і можуть бути підписані кількома залученими сторонами для підтвердження кожного етапу процесу [462, с. 14];

2. Системно-орієнтований chain of custody. Складність документування кожної взаємодії з доказами електронної форми спонукала до розроблення спеціалізованих систем, призначених для автоматизації та впорядкування процесу chain of custody, забезпечення цілісності доказів та їхньої допустимості в судовому процесі [310]. У цьому аспекті дослідники виділяють: chain of custody-центричні системи (підходи, що базуються на метаданих) та системи з інтегрованим chain of custody [462, с. 15]. Підходи на основі метаданих спрямовані на включення детальної інформації про докази в криміналістичні образи⁹, що підвищує цілісність chain of custody. Криміналістичні формати файлів, такі як Advanced Forensic Format 4 (AFF4), підтримують гнучкий збір метаданих, що допомагає документувати докази більш комплексно [362]. Системи з інтегрованим chain of custody впроваджені в системах управління доказами, таких як ERIN7, EvidenceOnQ, ChainLinx, Evidence Manager. Багато з цих систем присвоюють унікальні штрих-коди кожному доказу, що полегшує їх точне відстеження та опрацювання. Вони автоматизують процес chain of custody, генеруючи і записуючи позначки дати й часу для всіх дій, що зберігаються в постійному аудиторському журналі. Повний аудиторський журнал може бути відтворений як звіт chain of custody під час судового розгляду [462, с. 15];

3. Інфраструктурно керований chain of custody. Завдяки інтеграції криптографічних технологій, таких як цифровий підпис і сіре гешування [311], інфраструктурно керований chain of custody може використовувати весь потенціал цієї децентралізованої інфраструктури. Наприклад, останніми роками робилися різні спроби використати потенціал технології блокчейн для реалізації цього децентралізованого підходу для супроводу та збереження доказів електронної форми. Серед цих зусиль варто відзначити фреймворк chain of custody на основі Ethereum, запропонований S. Bonomi, M. Casini and C. Ciccotelli (2018) [321], який є яскравим прикладом у цьому контексті. Перехід до таких інфраструктурно орієнтованих методів помітно підвищив складність процесу chain of custody

⁹ Мова йде про криміналістичні образи електронних носіїв інформації, що виготовлені за результатами побітового копіювання.

порівняно з традиційними, простішими підходами. Однак це одночасно дало низку переваг, включаючи незмінність, прозорість, безпеку і децентралізацію [462, с. 16].

Nath S., Summers K., Baek J. and Ahn G.J. (2024) системно досліджують наведені підходи до chain of custody, аналізують їх переваги та недоліки та обґрунтовують потенційні можливості для вдосконалення та розвитку в цьому напрямі [462, с. 11-20], що може бути цікаво профільним спеціалістам, однак не висвітлюється нами з огляду на обмежений обсяг дисертаційного дослідження.

У світлі динамічного розвитку віртуальних технологій актуальними є дослідження, що стосуються ланцюга зберігання (chain of custody) для доказів електронної форми та існують в хмарному середовищі (Cloud Computing Environment).

Парадигма хмарних обчислень має багато переваг як для організацій, так і для приватних осіб. Однією з таких переваг є спосіб управління даними в хмарній інфраструктурі. Наприклад, дані розподіляються між різними центрами обробки даних для підвищення продуктивності та полегшення функцій балансування навантаження, масштабування та дедуплікації. Через це дані потребують ефективного індексування, щоб забезпечити їх пошук та оптимізацію, а також уникнути дублювання, яке часто призводить до зростання потреб у сховищах [451, с. 241].

Попри свої численні переваги, хмарні обчислення ставлять перед правоохоронцями та експертами з цифрової криміналістики значні виклики [383; 492; 414; 453; 485; 307; 503; 316; 446; 481]. Вони включають, але не обмежуються проблемами, пов'язаними з відсутністю стандартизації між різними політиками безпеки контенту, різними рівнями безпеки даних та їхніми угодами про рівень обслуговування, численними власниками, орендарями та юрисдикціями [312]. Як результат, правоохоронні органи повинні покладатися на місцеве законодавство, щоб мати можливість проводити збір доказів електронної форми [459]. Тому розбіжності в правових системах різних юрисдикцій у поєднанні з відсутністю співвідносності між Політиками безпеки контенту також створюють значні проблеми у контексті цифрової криміналістики [458]. У цьому сенсі відсутність

регулювання єдиного стандарту для обслуговування провайдерів хмарних послуг спонукала Європейський Союз (далі – ЄС) ініціювати зусилля з визначення мінімальних стандартів дотримання постачальниками послуг хмарних обчислень з метою створення механізмів для підтримки процесу розслідування в цьому середовищі [373; 451, с. 241].

Lucien L. (2024) узагальнює пропоновані дослідниками рішення для вирішення описаних вище викликів, що стоять перед ланцюгом зберігання (chain of custody) для доказів електронної форми та які існують у хмарному середовищі: методології та встановлені керівні принципи в підобластях цифрової криміналістики, щоб сформулювати конвергентні та дивергентні (де це можливо) настанови в напрямку єдиного загальноприйнятого керівництва для хмарних середовищ [309], ISO/IEC 27037:2012, керівні принципи National Institute of Standards and Technology (NIST) і нове регулювання ЄС, що створюють канал прямого співробітництва між судовими органами, зацікавленими в отриманні доказів, і провайдерами з ЄС [401; 371; 511], нові рамки та нові питання для оцінки під час проведення криміналістичних експертиз у хмарному середовищі [485; 307; 475]; нові концепції [440; 501; 307]; створення міжнародного суду для розв'язання питань, що стосуються різних юрисдикцій, забезпечення готовності Політики безпеки контенту щодо проведення судової експертизи [534; 451, с. 244].

Таким чином, ефективність використання доказів електронної форми в кримінальному провадженні безпосередньо залежить від наявності надійних механізмів забезпечення їхньої цілісності та автентичності. Центральним елементом цього процесу виступає концепція chain of custody (ланцюг збереження доказів), що об'єднує як технічні, так і процесуальні інструменти, спрямовані на ідентифікацію, збирання, здобуття, збереження, дослідження, аналіз та представлення доказів у спосіб, що унеможлиблює їх несанкціоновану зміну або підміну.

Процесуальні механізми, передбачені КПК України, зокрема вимоги до протоколювання, фіксації та способу ідентифікації, формують первинний рівень підтвердження цілісності цифрової інформації. Водночас відсутність чітко

визначених технічних процедур — таких як гешування, криміналістичне (побітове) копіювання, а також уніфікованих правил поводження з цифровими слідами — істотно знижує ефективність механізмів захисту доказів електронної форми від спотворення, втрати або фальсифікації.

ДСТУ ISO/IEC 27037:2017 пропонує уніфіковану модель поводження з доказами електронної форми та містить процедури їх ідентифікації, збирання, здобуття та збереження. При адаптації відповідних алгоритмів до умов кримінального провадження України слід враховувати специфіку національного правового регулювання, процесуальних гарантій та методів фіксації доказів. З огляду на зазначене, вбачається доцільним:

1. Розроблення та впровадження СОП для органів досудового розслідування, оперативних підрозділів, спеціалістів, експертів, прокурорів, які взаємодіють з доказами електронної форми. У цих СОП доцільно закріпити вимоги до ідентифікації, збирання, здобуття, збереження, дослідження, аналізу та представлення доказів електронної форми під час кримінального провадження.

2. Інтегрувати до СОП вимоги національних стандартів України у сфері інформаційної безпеки (зокрема, ДСТУ ISO/IEC 27037:2017, ДСТУ ISO/IEC 27001:2023, ДСТУ ISO/IEC 27002:2023), адаптувавши їх для потреб кримінального провадження.

3. Забезпечити закріплення chain of custody у відомчих документах органів досудового розслідування та прокуратури через визначення його сутності, базових принципів з подальшим розширенням на всіх суб'єктів кримінального процесу та впровадженням правових наслідків при порушенні процедур прозорості та відстежуваності при роботі з доказами досліджуваної категорії.

Таким чином, упровадження СОП, що охоплюють як правові, так і технічні вимоги до роботи з доказами електронної форми сприятиме забезпеченню належного підтвердження їх цілісності й автентичності та зміцненню процесуальних гарантій сторін кримінального провадження [94, с. 223-224].

2.3. Організаційні аспекти роботи з доказами електронної форми у кримінальному процесі України

Стрімкий розвиток цифрових технологій зумовив не лише появу нових джерел доказової інформації, а й висунув перед суб'єктами кримінального провадження низку нових викликів, пов'язаних з ідентифікацією, збиранням, збереженням, перевіркою та оцінкою доказів електронної форми. Ефективність роботи з доказами електронної форми значною мірою визначається не лише процесуальними умовами, але й організаційною спроможністю суб'єктів кримінального провадження. У цьому контексті важливою є оцінка стану організаційної готовності уповноважених органів до роботи з такими доказами, з урахуванням наявних інституційних моделей, кадрового забезпечення, матеріально-технічної бази та нормативної регламентації. Для з'ясування актуальних проблем практики у цій сфері було проведено емпіричне дослідження, результати якого дозволяють виокремити ключові проблемні зони, що потребують ефективного реагування.

У відповідь на питання «З якими проблемами Ви зіштовхуєтесь у роботі з доказами електронної форми?» респондентам пропонувалася можливість обрати кілька варіантів відповіді (та вказати власний варіант відповіді), за результатами чого визначено, що технічні аспекти зберігання доказів електронної форми (наявність носіїв інформації, захищених сейфів/кімнат тощо), є проблемою для 43% опитаних; технічна некомпетентність колег у питанні доказів електронної форми – 40%; використання доказів електронної форми в суді – 39%; процесуальна некомпетентність колег у питанні доказів електронної форми – 32%; безпека зберігання цифрових доказів – 30%; передача доказів електронної форми іншим органам /особам – 27%; використання доказів електронної форми в інших кримінальних провадженнях – 24%; тегування (виділення важливих ознак як дата, час, місце, сервіс отримання тощо для подальшого зручного пошуку) доказів електронної форми – 23%; відсутність достатньої кількості носіїв інформації, на які

здійснюється збереження інформації – 11% (див. Додаток Б, Додаток В Рис. 10) [114, с. 86-87].

Для з'ясування проблем, що найчастіше виникають при збиранні, перевірці та оцінці доказів електронної форми респондентам також було запропоновано надати розгорнуті відповіді, за результатом аналізу та групування яких встановлено такі потенційно проблематичні напрями як: підтвердження цілісності та незмінності доказів – 18%; технічні – 13%; некомпетентність власна або інших / відсутність знань – 12%; відсутність або зайнятість спеціалістів – 12%; під час пошуку та фіксації – 12%; неналежне збирання та фіксація під час досудового розслідування – 11%; збереження та зберігання – 9%; використання в суді – 8%. При цьому у 21% опитаних вказують про відсутність проблемних питань. Різні категорії респондентів у відповідях вказували специфічні питання, зокрема на відсутність спеціалістів вказували переважно слідчі / детективи та прокурори, підтвердження цілісності та незмінності доказів – переважно судді та прокурори; а на неналежне збирання та фіксація під час досудового розслідування – переважно прокурори.

Результати проведеного нами опитування суб'єктів кримінального провадження ілюструють зосередженість проблемних питань практиків під час роботи з доказами електронної форми не на недоліках КПК України (щодо необхідності визначення понять чи виокремлення нового процесуального джерела доказів), а переважно на організаційних аспектах [114, с. 85-89].

Насамперед необхідно вказати, що організаційна готовність суб'єктів кримінального провадження до роботи з доказами електронної форми є важливим чинником ефективності процесу їх ідентифікації, збирання, здобуття, збереження, дослідження, аналізу та представлення. Досліджувана здатність суб'єктів кримінального провадження безпосередньо залежить від: 1) рівня матеріально-технічного забезпечення суб'єктів кримінального провадження, наявності спеціалізованого обладнання та належної інфраструктури; 2) кадрової спроможності органів досудового розслідування, прокуратури, суду та інших учасників кримінального провадження з-поміж державного сектору; 3) наявності в

суб'єктів кримінального провадження нормативної основи (норми кримінального процесуального законодавства, закони та підзаконні НПА, відомчі інструкції та регламенти тощо) щодо роботи під час кримінального провадження з доказами електронної форми.

Щодо матеріально-технічного забезпечення суб'єктів кримінального провадження, наявності спеціалізованого обладнання та належної інфраструктури насамперед йдеться про забезпечення органів досудового розслідування цифровими криміналістичними інструментами, що дозволяють здійснювати роботу з доказами електронної форми відповідно до ДСТУ ISO/IEC 27037:2017. До таких належать пристрої write-blocker (апаратні засоби блокування запису), forensic workstations (криміналістичні робочі станції), ПЗ для створення та аналізу криміналістичних образів (FTK, EnCase, X-Ways Forensics), системи гешування та перевірки цілісності даних. Наявність в органів досудового розслідування відповідних технічних і програмних засобів для роботи з доказами електронної форми є критично необхідною умовою здійснення результативних слідчих (розшукових) дій [110, с. 260].

Кадрова спроможність органів досудового розслідування, прокуратури, суду та інших учасників кримінального провадження є наступною складовою організаційної готовності суб'єктів кримінального провадження до роботи з доказами електронної форми. Кадрове забезпечення роботи з доказами електронної форми під час кримінального провадження виступає одним із ключових елементів ефективності досудового розслідування у цифровому середовищі. Специфіка таких доказів обумовлює потребу у міждисциплінарній компетенції осіб, які залучаються до роботи з ними. До цього кола належать оперативні працівники, слідчі, детективи, прокурори, спеціалісти, експерти та навіть судді.

Одним із системних викликів для ефективного кримінального провадження, пов'язаного з використанням доказів електронної форми є істотний дефіцит фахових знань у суб'єктів кримінального провадження. Відсутність належного рівня спеціалізованої підготовки у сфері цифрових технологій безпосередньо впливає на здатність ідентифікувати, вилучати, аналізувати й правильно

інтерпретувати цифрову інформацію під час кримінального провадження. Зокрема, слід констатувати брак розуміння базових технічних понять, таких як структура цифрового сліду, механізми гешування, процедурне значення криміналістичної (побітової) копії, а також способи відновлення видалених або пошкоджених даних. Також на практиці нерідко фіксується нерозуміння ролі метаданих та їх значення для підтвердження автентичності даних та хронологічної послідовності подій. В окремих випадках слідчі не володіють навичками первинного огляду цифрового пристрою без ризику порушення цілісності даних [110, с. 260].

Крім того, певна частина слідчих, прокурорів та суддів не володіє знаннями щодо технічних та процесуальних аспектів подолання логічного захисту, таких як дешифрування, доступ до хмарних ресурсів, робота з віртуальними середовищами, застосування спеціалізованого ПЗ. Це нерідко призводить до порушення процедури вилучення й зберігання даних, прийняття помилкових процесуальних рішень, що надалі може вплинути на допустимість відповідного доказу.

Технічна некомпетентність суб'єктів кримінального провадження (стосується всіх представників) потенційно є чинником недооцінки або переоцінки доказу, що може мати суттєві негативні наслідки для кримінального провадження. Як на рівні КПК України, так і підзаконних НПА фактично не встановлено уніфікованих кваліфікаційних вимог до осіб, котрі здійснюють первинний контакт з цифровими носіями, зокрема під час обшуку або тимчасового доступу. Це створює ризики неналежної фіксації цифрової інформації, втрати або зміни її змісту, що, своєю чергою, може призвести до порушення його цілісності та втручання у зміст та визнання доказу подальшому недопустимим. Брак профільної підготовки, сертифікацій або програм підвищення кваліфікації суб'єктів, які фактично залучаються до роботи з доказами електронної форми залишається однією з суттєвих прогалин у кадровій політиці більшості органів досудового розслідування.

Додатково спостерігається суттєвий дисбаланс у професійному рівні та технічній підготовленості між підрозділами різних відомств: тоді як окремі спеціалізовані підрозділи НАБУ, Департаменту Кіберполіції Національної поліції

України або СБУ демонструють високий рівень компетентності, регіональні слідчі підрозділи деяких ОДР часто не мають елементарної експертизи чи кадрового ресурсу для роботи з доказами досліджуваної форми. Очевидною є проблема навіть на рівні практики вилучення електронних носіїв інформації, яка суттєво різниться у різних органів досудового розслідування та навіть регіональних «традицій», обумовлених позиціями апеляційних судів відповідних областей. Уніфікація кваліфікаційної підготовки представників органів досудового розслідування та прокурорів (такі тренінги авторка систематично проводить у Тренінговому центрі прокурорів України з січня 2021 року) до роботи з доказами електронної форми відповідно до вимог ДСТУ ISO/IEC 27037:2017 є очевидною та навіть перезрілою з огляду на час запровадження цього стандарту – з січня 2019 року [110, с. 261].

Одним з надзвичайно актуальних на сьогодні питань для кадрового забезпечення ОДР є підготовка фахівців з розвідки на основі відкритих джерел або ж Open Source Intelligence (OSINT) [116]. В умовах цифрової трансформації джерел інформації інструменти OSINT набувають дедалі більшого значення в діяльності органів досудового розслідування. OSINT розвідка дозволяє оперативно отримувати інформацію з відкритих джерел, зокрема соціальних мереж, інтернет-форумів, публічних баз даних, ЗМІ, сервісів архівування вебсторінок, доменних реєстрів тощо. Принциповим є те, що інформація здобувається без порушення конфіденційності шляхом обробки загальнодоступних відомостей, що відкриває перспективи її використання в межах кримінального провадження.

Класифікація інструментів OSINT передбачає поділ за функціональним призначенням: платформи візуального зв'язування інформації (наприклад, Maltego), системи багатоканального пошуку й моніторингу (наприклад, SpiderFoot, Recon-ng), сервіси архівування вмісту вебсторінок (Archive.today, Wayback Machine - інтернет-архіви, що зберігають копії вебсторінок у різні моменти часу), трекери доменних імен (WhoisXML, DNSdumpster), аналіз соціальних графів (Social Links, SOCMINT-аналітика) тощо. Ці інструменти дозволяють ідентифікувати цифрові сліди, зв'язки між акаунтами, часові відмітки активності, IP-адреси, метадані тощо – тобто інформацію, яка потенційно може стати доказом.

Ефективна робота з відповідними інструментами вимагає системного навчання та постійного підвищення кваліфікації. Тут важливим є також впровадження стандартів Протоколу Берклі в роботу ОДР, що передбачає відповідну підготовку працівників.

Отже, уніфікація підходів до кадрового забезпечення, таких як створення спеціалізованих структурних підрозділів (наприклад, криміналістичних ІТ-лабораторій), міжвідомчого переліку профільних посад і кваліфікаційних вимог до суб'єктів кримінального провадження, які взаємодіють з доказами електронної форми (внутрішньовідомча сертифікація) – це нагальна потреба для забезпечення адекватної роботи суб'єктів кримінального провадження в досліджуваному питанні.

Уже зараз недоліки кадрової спроможності можна компенсувати шляхом створення сталої інституційної системи підготовки, підвищення кваліфікації та сертифікації суб'єктів кримінального провадження, які залучені до роботи з доказами електронної форми. Ідеться як про слідчих, прокурорів і суддів, так і про експертів, спеціалістів, оперативних працівників, на яких покладено обов'язки з ідентифікації, вилучення, зберігання та дослідження цифрової інформації.

Одним з ключових напрямів удосконалення є розроблення та впровадження міжвідомчих програм професійного навчання, орієнтованих на цифрову криміналістику, з урахуванням специфіки кримінального процесуального законодавства України, міжнародних стандартів, а також галузевих особливостей (наприклад, щодо кіберзлочинів, торгівлі людьми, воєнних злочинів тощо). Відповідні тренінгові програми мають передбачати як теоретичну частину, так і практичні модулі роботи з цифровими носіями інформації, застосування спеціалізованого ПЗ, документування процесуальних дій з дотриманням вимог щодо забезпечення цілісності доказів електронної форми.

Окремої уваги заслуговує потреба в інтеграції цифрової грамотності до освітніх програм правничих навчальних закладів, що забезпечить формування первинної компетентності майбутніх фахівців щодо доказів електронної форми їх властивостей та правового статусу в межах кримінального процесу.

Третім компонентом організаційної готовності суб'єктів кримінального провадження є наявність нормативних засад (норми кримінального процесуального законодавства, закони та підзаконні НПА, відомчі інструкції та регламенти тощо) щодо роботи під час кримінального провадження з доказами електронної форми [110, с. 261]. Важко переоцінити необхідність забезпечення належного правового регулювання питання доказів електронної форми в КПК України. У межах діяльності окремих відомств (зокрема НАБУ) існують внутрішні інструкції, що регламентують алгоритми дій при роботі з цифровими носіями та комп'ютерними даними. Ці документи, як правило, мають обмежений доступ і застосовуються в межах певного відомства.

Однак ключовою проблемою є брак спільного для всіх органів досудового розслідування уніфікованого стандарту, який регламентував би мінімально необхідні вимоги до дій усіх правоохоронних органів під час роботи з доказами електронної форми та який би був визначений як обов'язковий до використання. Така фрагментарність регламентації унеможливорює формування єдиної практики правозастосування.

Додатково варто зазначити, що більшість відомчих матеріалів лише точково регулюють питання роботи з певним видом пристроїв або стосуються специфічних ситуацій та лише частково враховують положення ДСТУ ISO/IEC 27037:2017 або Протоколу Берклі.

Одним із ключових шляхів методологічного забезпечення суб'єктів кримінального провадження в досліджуваному напрямі є методичні рекомендації [32; 31; 30; 25; 161; 25]. На нашу думку, використання розрізнених методичних рекомендацій як інструменту вдосконалення знань суб'єктів кримінального провадження щодо роботи з доказами електронної форми під час кримінального провадження неефективне через брак цілісного теоретичного розуміння окресленої теми й концептуального підходу до їх процесуальної оцінки. Ось чому перспективним напрямом є розроблення та впровадження єдиних для всіх суб'єктів кримінального провадження СОП щодо роботи з доказами досліджуваної категорії [110, с. 261].

Організаційна готовність суб'єктів кримінального провадження до роботи з доказами електронної форми передбачає забезпечення рівних матеріально-технічних можливостей, наявності спеціалізованих підрозділів та фахових кадрів у їх структурі (для забезпечення фахової комунікації), а також застосування спільних для всіх науково обґрунтованих і технологічно оптимізованих підходів до такої роботи. Все це є передумовою ефективної взаємодії між суб'єктами кримінального провадження під час роботи з доказами електронної форми. Досі питання залишається дискусійним, що спонукало нас звернутися до самих суб'єктів правозастосування.

Для з'ясування рівня взаємодії між суб'єктами правозастосування щодо пошуку доказів електронної форми респондентів запитали, чи виникає у їх роботі необхідність звертатись до колег для пошуку доказів електронної форми. 54% респондентів вказують, що не мають такої потреби, 37% стверджують про таку необхідність з них 3% додатково конкретизують, що звертаються для цього до фахівців. Ще 7% вказують, що звертаються до працівників підрозділів кіберполіції. Також 2% респондентів (19 осіб), всі з яких є працівниками кіберполіції, відповіли, що вони і є тими колегами, до яких звертаються за допомогою в пошуку доказів електронної форми (див. Додаток Б, Додаток В Рис. 9). З огляду на те, що 37% респондентів вказують на необхідність звертатись до колег для пошуку доказів електронної форми (більш як 2/3 з цих 37% є прокурорами), така потреба вимагає вирішення або шляхом створення й розширення штатів профільних спеціалістів, або ж шляхом навчання прокурорів самостійно шукати та фіксувати докази досліджуваної категорії [114, с. 88].

Серйозним прикладом ефективної організації роботи з доказами електронної форми під час кримінального провадження є досвід НАБУ в частині створення у своїй структурі криміналістичної ІТ-лабораторії зі штатом відомчих спеціалістів, які організаційно не підпорядковані керівнику органу досудового розслідування, є процесуально незалежними та можуть залучатися до слідчих дій для реалізації процедур, визначених ДСТУ ISO/IEC 27037:2017.

З розвитком ІТ людське спілкування отримало новий інструмент у вигляді таких програм передачі повідомлень. Кількість інформації в електронній формі почала зростати поступово, а потім в геометричній прогресії. І правоохоронці одразу зрозуміли, що цю інформацію можна збирати як докази для розслідування злочинів. Яким чином відповіла на ці зміни правоохоронна система? Найбільша за кількістю правоохоронців – поліція, з середини 2000-х років почала створити можливості для збирання та дослідження доказів електронної форми створюючи в штаті поодинокі посади ІТ-експертів. Трішки раніше Міністерство юстиції України сформувало напрям комп'ютерно-технічних досліджень. Слідчі вилучали комп'ютерну техніку та телефони, направляли їх на експертизу та чекали висновків. На якомусь етапі такий підхід працював, однак відсутність в експертів належного технічного обладнання та спеціалізованого ПЗ не сприяла розвитку відповідної сфери [47, с. 72–73].

З прийняттям у 2012 році чинного КПК України не вдалось ефективно врегулювати ні питання доказів електронної форми ні ефективного проведення їх досліджень. Системна проблема спостерігалась уже на початку 2010-х років коли слідчий міг чекати на висновки експерта місяці, а то й рік. Саме такою була ефективність роботи з доказами електронної форми. Утім, за останні 10 років цю проблему системно не вирішено. Процесуальна традиція поки що перемагає, топуправлінці зі сфери кримінальної юстиції й гадки не мають, що з цим робити, а можливо не знають, що взагалі є проблема зі збиранням органами досудового розслідування доказів електронної форми[47, с. 73]. Це питання, на жаль, досі не стало стратегічним на порядку денному вищого менеджменту правоохоронної системи України.

Водночас варто вказати про приклад ефективної роботи НАБУ у цьому напрямі. У 2015 році створено НАБУ, яке не має у своєму складі експертної установи, а кримінальні провадження складні, абсолютна більшість розслідується в ретроспективі. Злочини вчинені давно, потенційні правопорушники часто самі є кваліфікованими юристами та не схильні надавати покази, знайдені та вилучені документи далеко не завжди вказують на винних. На самому старті менеджментом

НАБУ за порадою міжнародних партнерів прийнято рішення створити криміналістичну ІТ-лабораторію для роботи з доказами електронної форми. Враховуючи абсолютну відсутність можливості дотримання усталеної процесуальної традиції по роботі з доказами електронної форми шляхом призначення експертизи, в Управлінні аналітики та обробки інформації НАБУ розробили концепцію роботи з доказами електронної форми в новому процесуальному форматі, яка ніколи до цього широко і системно не використовувалася – залучати спеціаліста ІТ-криміналіста до проведення огляду речей та документів, замість призначення експертизи. Ретельним системним аналізом процесуальних норм встановлено, що самі по собі пошук, виявлення, фіксація інформації на електронних носіях не є винятковою прерогативою експертизи як форми застосування спеціальних знань. Щобільше, експертиза може дати висновок, який ґрунтуються на спеціальних знаннях експерта, а констатація факту наявності інформації – це просто очікуваний результат прогнозованої послідовності технічних дій, які частково можна виконати автоматизовано. Саме таким чином з самого початку запуску у 2015 році побудована робота криміналістичної ІТ-лабораторії НАБУ. Чотирьом фахівцям ІТ-лабораторії (станом на 2021 рік) вдавалося задовольняти попит понад 200 детективів. Фахівці відділу беруть участь як у слідчих діях, під час яких первинно збираються докази (тобто викорюють роль DEFR – прим. авт.) електронної форми так і досліджують їх разом із детективами під час проведення слідчих оглядів в лабораторних умовах. Крім того, ІТ-лабораторія є осередком поширення базових знань по роботі з доказами електронної форми для детективів НАБУ [47, с. 73–74].

Варто звернути увагу, що КПК України в ч. 2 ст. 168 КПК України суттєво обмежує сторону обвинувачення у можливості вилучення ЕІС, КС, МТСЗ. Наприклад, абз. 3 ч. 2 ст. 168 КПК України передбачає можливість вилучення ЕІС, КС, МТСЗ, якщо такі об'єкти отримані в результаті вчинення кримінального правопорушення чи є засобом або знаряддям його вчинення. Тобто вже на місці

проведення обшуку треба провести пошук інформації, яка про це може свідчити. Зазвичай без спеціаліста ефективно провести такі дії фактично неможливо.

Також необхідно врахувати, що з 2015 року діє норма абз. 2 ч. 2 ст. 168 КПК України щодо можливості вилучення комп'ютерів та телефонів лише як тимчасово вилученого майна. До того ж клопотання про накладення арешту має бути направлено до слідчого судді протягом 48 годин після вилучення такого майна. Ця законодавча вимога ставить орган досудового розслідування у становище, коли він змушений у парадоксально короткий строк дослідити вилучені речі на предмет наявності підстав для накладення арешту. Очевидно, що за 48 годин висновки експертиз, наприклад, щодо 10 комп'ютерів та 10 телефонів отримати неможливо. У цьому разі лише залучення спеціаліста ІТ-криміналіста дозволяє виконати майже непосильні вимоги законодавця [47, с. 74–75].

І наостанок, сам законодавець ніби підштовхує органи досудового розслідування до практики залучення спеціалістів ІТ-криміналістів. Зокрема, відповідно до ч. 4 ст. 99 КПК України копії інформації, що міститься в інформаційних системах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа. Таким чином, орган досудового розслідування може забезпечити результативне проведення слідчих (розшукових) дій в частині отримання інформації, що міститься в інформаційних системах, як при вилученні електронних носіїв інформації, так і при виготовленні копії такої інформації у порядку абз. 4 ч. 2 ст. 168 КПК України, що визнається судом як оригінал документа. У цьому разі складно переоцінити роль спеціаліста, що може забезпечити технічний аспект процесу копіювання інформації з урахуванням положень ДСТУ ISO/IEC 27037:2017, гарантуючи цілісність інформації [47, с. 75].

На наше переконання, ефективне проведення досудового розслідування значної частини кримінальних правопорушень потребує залучення ІТ-криміналістів як спеціалістів (у порядку ст. 71 КПК України). Процесуальні традиції та звичаї в частині роботи з доказами електронної форми доцільно переосмислити, залучаючи експертів лише щодо складних питань, що вимагають

відповідного висновку. Саме так зроблено, наприклад, в Німеччині, де компетенція ІТ-криміналістів та ІТ-експертів розділені, де спеціалісти ІТ-криміналісти функціонально наближені до слідчих підрозділів, як це зроблено у НАБУ [47, с. 75]. Враховуючи викладене, пропонуємо розглянути можливість створення в структурі всіх правоохоронних органів підрозділів ІТ-криміналістів, котрі зможуть забезпечити ефективну роботу з доказами електронної форми під час кримінального провадження.

Поряд з організаційною готовністю системи кримінальної юстиції до ефективної роботи з доказами електронної форми надзвичайно актуальним є питання зберігання доказів електронної форми та контролю доступу до них. Зберігання електронних носіїв інформації у межах кримінального провадження вимагає дотримання суворих технічних параметрів, що забезпечують збереження їх цілісності та автентичності інформації. Цей процес охоплює як фізичне зберігання електронних носіїв інформації, так і створення та архівацію криміналістичних образів (побітових копій), резервних копій, вимоги до транспортування тощо. З огляду на високу чутливість цифрових даних до зовнішніх чинників, одним із ключових технічних аспектів є забезпечення контрольованого середовища з регульованими температурними й показниками вологості, ізоляцією від електромагнітного випромінювання та захистом від механічного або статичного ураження. Технічні вимоги до зберігання електронних носіїв інформації під час кримінального провадження на разі законодавцем не встановлені. Водночас окремі аспекти визначено в ДСТУ ISO/IEC 27037:2017. Національні НПА та методичні рекомендації наразі не охоплюють у повному обсязі всі аспекти поводження з доказами електронної форми [110, с. 263].

У зв'язку з актуальними викликами, зокрема загрозами кібератак та ризиками втрати інформації через технічні збої, особливої ваги набуває ідея створення централізованого відомчого віртуального сховища для резервного зберігання доказів електронної форми. Таке сховище має бути ізольованим від загальних мереж, підтримувати систему регулярного бекапування, а також передбачати можливість довготривалого зберігання інформації на стрічкових носіях (tape

storage), які мають підвищений захист від логічного знищення або шифрування у разі зовнішнього втручання. Реалізація такої моделі підвищила б рівень цифрової безпеки кримінального провадження в умовах гібридних загроз і сприяла б формуванню єдиної системи роботи з доказами електронної форми. Водночас вже сьогодні актуалізується питання деградації електронних носіїв інформації, що використовуються для зберігання доказів електронної форми під час кримінального провадження, що створює загрозу їх цілісності. Фізична та логічна деградація носіїв даних є однією з малодосліджених, проте критично важливих загроз для цілісності, а отже, і доказової цінності цифрової інформації під час кримінального провадження. На відміну від традиційних матеріальних носіїв (паперу чи фізичних предметів), цифрові носії інформації схильні до руйнування їх фізичного середовища з плином часу, технічної нестабільності та деградації, що може спричинити часткову або повну втрату інформації навіть без зовнішнього впливу [110, с. 263].

Флешнакопичувачі (USB, SD-карти) характеризуються обмеженою кількістю циклів запису/зчитування, високою чутливістю до температурних коливань та електростатичних розрядів. Магнітні носії, зокрема жорсткі диски (HDD), схильні до деградації внаслідок демагнетизації, механічного зносу обертальних елементів та утворення «bad sectors». Оптичні диски (CD, DVD), хоч і тривалий час вважалися архівними носіями, втрачають свою надійність через розшарування, деградацію полімерних шарів або подряпини, які унеможливають зчитування даних. У відповідь на ці загрози необхідним вважаємо впровадження носіїв, орієнтованих на довготривале зберігання: спеціалізовані SSD з низьким рівнем зношення, WORM-системи (write once, read many), які не допускають перезапису, а також «холодне» архівування — зберігання носіїв у контрольованому середовищі з обмеженим доступом і періодичним дублюванням вмісту. Застосування подібних носіїв може бути виправданим у випадках, коли цифрова інформація повинна зберігатися багато років до моменту її дослідження у суді.

Але сьогодні величезна кількість доказів електронної форми зберігається на електронних носіях інформації у формі флешнакопичувачів (USB, SD-карти), що

мають високі ризики деградації даних та втрати доказу. Досвід практичної роботи свідчить, що оригінальні носії з плином часу виходять з ладу, що своєю чергою робить неможливим дослідження їх змісту під час судового розгляду. Зокрема, це стосується флешкарт пам'яті типу microSD/SD, USB-флешнакопичувачів та оптичних дисків. У практичних ситуаціях більшість таких випадків пов'язана із заводським браком та/або низькою якістю виробництва носіїв, часом це наслідок випадкових подій або умисних дій третіх осіб. Ось чому від держателя цього доказу (слідчого, прокурора, судді тощо) вимагається вживати заходів щодо збереження цілісності даних і можливості їх подальшого використання під час кримінального провадження. Відповіддю на цей виклик є запровадження сталої практики виготовлення резервних копій доказів електронної форми. Законодавець передбачив можливість існування резервних копій оригінальних примірників технічних носіїв інформації зафіксованої процесуальної дії та можливість їх зберігання поза матеріалами кримінального провадження (ч. 3 ст. 107 КПК України). Допустимість резервного носія та копій комп'ютерних даних, які на ньому зберігаються, визначається ч. 3 ст. 99, п. 1 ч. 5 ст. 99 КПК України, при цьому зміст оригінального носія (документа, що має бути наданий суду) підтверджується копіями комп'ютерних даних (відомостями), зафіксованими на резервному носії. У судовому провадженні під час дослідження судом копій комп'ютерних даних на резервних носіях можуть виникнути обставини, коли цілісність, а відповідно й достовірність копій комп'ютерних даних може бути поставлена під сумнів стороною захисту. У такому разі прокурор має бути готовий підтвердити вірогідність цих копій. Порівнявши геш-код, установлений з копії даних резервного носія методом обчислення, зі значенням, зафіксованим у протоколі, можна гарантовано довести чи спростувати достовірність копій комп'ютерних даних резервного носія [44, с. 43-47].

Ще одним важливим аспектом досліджуваного нами питання зберігання доказів є контроль доступу до доказів електронної форми.

Контроль доступу до доказів електронної форми в кримінальному провадженні є критичним елементом гарантування їхньої цілісності та правдивості

і важливим аспектом забезпечення chain of custody. Правове регулювання цього процесу вимагає чіткого розмежування повноважень суб'єктів кримінального процесу, забезпечення технічної захищеності інформації та відповідності дій встановленому алгоритму chain of custody. Розмежування доступу здійснюється відповідно до процесуальних ролей. Слідчий, як ініціатор слідчих дій, відповідає за тимчасове зберігання електронних носіїв інформації та організацію доступу до інформації. Його завдання полягає не лише у виявленні та вилученні електронних носіїв інформації, а й у забезпеченні безпечного їх функціонального обігу. Прокурор виконує контрольну функцію, приймаючи рішення щодо правомірності та необхідності доступу до інформації, у тому числі оцінюючи обсяг і межі втручання в особисту сферу. Захисник реалізує право на ознайомлення із зібраними доказами відповідно до ч. 2 ст. 290 КПК України, однак таке ознайомлення не повинно ставити під загрозу конфіденційність персональної інформації інших осіб, що міститься на носіях, які вилучені під час кримінального провадження. У цьому контексті особливе значення має чітке визначення обсягу доступної інформації. Експерт або технічний спеціаліст отримує доступ до цифрової інформації або до електронних носіїв інформації винятково в межах наданого процесуального доручення (ухвали суду або постанови прокурора чи слідчого) і не має права виходити за межі завдання, визначеного для проведення експертного дослідження.

У цьому аспекті актуальними є різновиди сучасних програмних рішень, що містять інтегровані алгоритми chain of custody (Більше про це див. 2.2). Такі технічні засоби контролю мають відповідати сучасним стандартам інформаційної безпеки. У кримінальному провадженні доцільне використання багаторівневих систем доступу, які забезпечують різний рівень повноважень для слідчого, прокурора, захисника, експерта. Автентифікація користувачів через двофакторні механізми, токени або цифрові сертифікати дозволяє встановити індивідуальну відповідальність за кожен сеанс доступу. Надзвичайно важливою є система журналювання, яка фіксує усі дії з доказами електронної форми — перегляд, копіювання, зміни — із зазначенням точного часу, ідентифікатора пристрою та IP-адреси. Логування змін у метаданих (зокрема, часу створення, останнього доступу,

модифікації файлів) дає змогу ідентифікувати будь-які несанкціоновані втручання або спроби прихованої маніпуляції даними.

З огляду на викладене, перспективним напрямом є запровадження уніфікованої цифрової платформи для забезпечення контролю доступу до доказів електронної форми. Така платформа має базуватись на цифровій ідентифікації учасників провадження, з обов'язковим журналюванням усіх дій у межах електронної справи. Централізована система управління доступом із можливістю призначення ролей та рівнів дозволів, а також обов'язковий аудит усіх взаємодій з доказами в рамках chain of custody, дозволить мінімізувати ризики фальсифікації та забезпечити дотримання принципу належної правової процедури. Запровадження таких технічних і організаційних рішень потребує відповідного процесуального оформлення та нормативного закріплення.

Важливим питанням, яке пов'язане з контролем доступу до доказів, але перебуває в етичній площині, є обмеження доступу до інформації, міститься на носіях, які вилучені під час кримінального провадження, однак не має доказового значення і належить до персональної інформації інших осіб. Йдеться передусім про чутливу інформацію: особисте листування, приватні фотографії, відеозаписи, медичні або фінансові дані, а також відомості, що становлять комерційну таємницю третіх осіб. У певних випадках така інформація не пов'язана з обставинами кримінального правопорушення, однак через технологічну невіддільність від пристрою, що, наприклад, вилучений під час обшуку, вона виявляється доступною як для сторони обвинувачення, так і для сторони захисту під відкриття матеріалів досудового розслідування [110, с. 264-265].

Правова конструкція, передбачена ч. 2 ст. 290 КПК України, покладає на сторону обвинувачення обов'язок надати іншій стороні доступ до всіх матеріалів досудового розслідування, у тому числі до копій документів – сюди ж належать всі комп'ютерні дані, всі відомості з вилучених електронних носіїв інформації та виготовлені копії цифрових даних з пристроїв, що оглядалися. Водночас чинне законодавство не містить механізму обмеження доступу до інформації, що була виявлена та збережена, але не включена до переліку доказів у провадженні. Це

створює потенційну загрозу порушення права на повагу до приватного життя, особливо у випадках, коли відомості про інтимне, особисте або конфіденційне передаються на носіях у межах відкриття матеріалів стороною обвинувачення.

Таким чином, процесуальне регулювання доступу до інформації, що не має доказового значення, необхідно уточнити із урахуванням вимог пропорційності, мінімізації втручання та спеціального режиму обробки чутливих персональних даних, вилучених у межах кримінального провадження.

Розгляд організаційних аспектів роботи з доказами електронної форми у кримінальному процесі України засвідчив наявність низки суттєвих викликів, пов'язаних із неузгодженістю нормативно-правового регулювання, технологічною невідповідністю інфраструктури органів досудового розслідування, а також недостатньою підготовленістю персоналу. Емпіричні дані свідчать про фрагментарність і нерівномірність організаційної спроможності різних суб'єктів кримінального провадження щодо роботи з доказами електронної форми.

Установлено, що в умовах цифровізації суспільства забезпечення ефективного функціонування механізмів збирання, обробки, збереження та використання доказів електронної форми вимагає системного вдосконалення організаційної моделі взаємодії між підрозділами, стандартизації процедур, а також адаптації кадрів до нових технологічних умов. Відсутність єдиного уніфікованого алгоритму дій, недостатній рівень технічного оснащення та низький рівень спеціалізованої підготовки працівників створюють загрози для забезпечення цілісності та автентичності доказів електронної форми.

РОЗДІЛ 3. ПРОЦЕСУАЛЬНІ ПОВНОВАЖЕННЯ ТА ФУНКЦІОНАЛЬНІ РОЛІ СУБ'ЄКТІВ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ У ВЗАЄМОДІІ З ДОКАЗАМИ ЕЛЕКТРОННОЇ ФОРМИ

3.1. Слідчий як суб'єкт роботи з доказами електронної форми в кримінальному провадженні

У контексті розслідування кримінальних правопорушень, що супроводжуються цифровими слідами, особливого значення набуває релевантна компетентність осіб, уповноважених на проведення досудового розслідування — дізнавача, слідчого та детектива (надалі — слідчий — задля уникнення повторного називання всіх трьох суб'єктів). Саме ці суб'єкти зазвичай перші взаємодіють зі слідами кримінального правопорушення, і від їхньої кваліфікації, рішень та дій залежить подальша доля здобутих доказів і процесуальна допустимість останніх.

Слідчий у межах кримінального провадження наділений повноваженнями, що дозволяють проводити за власною ініціативою, а також ініціювати проведення слідчих (розшукових) дій та НСРД, спрямованих на виявлення та фіксацію доказів електронної форми. В окремих випадках слідчий самостійно визначає потенційні джерела цифрової інформації, орієнтуючись на загальні обставини події кримінального правопорушення. Слідчий повинен мати не лише юридичні, але й базові технічні знання щодо природи цифрової інформації, віртуального середовища та сучасних технічних пристроїв, володіти хоча б мінімальними навичками проведення OSINT. Технічна освіченість слідчого сприятиме усвідомленню власних спроможностей щодо реалізації технічних процесів та доцільності залучення спеціаліста (ст. 71 КПК України) у сфері цифрової криміналістики для проведення слідчих (розшукових) дій з потенційними цифровими об'єктами.

У частині фіксації доказів ключовим етапом є точне відображення виявлених електронних носіїв інформації чи комп'ютерних даних у протоколах слідчих (розшукових) дій, де мають бути належно відображені технічні аспекти проведення

відповідної слідчої (розшукової) дії, характеристики інформаційних систем чи електронних носіїв інформації, способи ідентифікації комп'ютерних даних тощо. Належне фіксування доказу електронної форми, є запорукою підтвердження його цілісності, надання суду достовірного уявлення про умови його виявлення та процес взаємодії з суб'єктами кримінального провадження (chain of custody). Реалізація цього аспекту вимагає обізнаності з ДСТУ ISO/IEC 27037:2017 і розуміння його ролі в процесі фіксації доказів досліджуваної категорії.

Таким чином, процесуальна ініціатива слідчого щодо роботи з доказами електронної форми становить важливий компонент ефективної роботи з ними. В умовах відсутності в КПК України та відомчих НПА чітко встановлених технічних процедур, ризики втрати доказів досліджуваної категорії можуть бути усунуті шляхом індивідуальної ініціативи слідчого щодо покращення власних знань у цій сфері та застосування визначених ДСТУ ISO/IEC 27037:2017 процедур, а в перспективі – шляхом комплексної методичної стандартизації.

Організаційна складова роботи слідчого з доказами електронної форми є не менш значущою за процесуальну. Вона охоплює питання належного поводження з електронними носіями інформації, взаємодії зі спеціалістами у сфері цифрової криміналістики, забезпечення збереження цифрового середовища, документування процесу обробки даних тощо.

Слідчий найчастіше має справу з технічними пристроями та електронними носіями інформації як потенційними джерелами доказів під час обшуку та огляду. Відповідно до пункту 5.4 ДСТУ ISO/IEC 27037:2017 процес обробки доказів електронної форми включає: ідентифікацію (identification), збирання (collection), здобуття (acquisition) та збереження (preservation). З урахуванням практики проведення слідчих (розшукових) дій наведені елементи процесу роботи з доказом електронної форми не є послідовними (і навіть обов'язковими) етапами й повинні реалізовуватись одночасно. Тож окреслимо умовні етапи роботи слідчого з доказами електронної форми щодо технічних пристроїв та електронних носіїв інформації, з урахуванням норм КПК України: 1) виявлення під час слідчої (розшукової) дії та встановлення наявності відомостей, що мають значення для

кримінального провадження; 2) ідентифікація характеристик пристрою (марка, модель, серійний номер, тип з'єднання, наявність зовнішніх носіїв) та їх відображення в протоколі слідчої (розшукової) дії; 3) вилучення пристрою та (або) виготовлення копії даних; 4) фіксація в протоколі, пакування та долучення до матеріалів кримінального провадження; 5) зберігання для подальшого дослідження.

3-поміж етапів роботи з доказами електронної форми першорядним є визначення правомірного способу отримання інформації, адже перед слідчим постає необхідність прийняття рішення, а фактично вибір між фізичним вилученням технічного пристрою, електронного носія інформації або ж експрес-переглядом, подоланням логічного захисту (за потреби) та копіювання інформації. Такий вибір слід робити на основі аналізу низки факторів — процесуальних обмежень, доступних стороні обвинувачення технічних можливостей, способів зберігання інформації, оперативної обстановки, а також поведінки власника технічного пристрою. З метою забезпечення належної правової процедури й допустимості доказів у кримінальному провадженні доцільно запропонувати слідчим (а також прокурорам та іншим особам, що залучені до відповідних процесів) алгоритм підходів до оцінки ситуації на місці проведення слідчої (розшукової) дії та прийняття слідчим (або прокурором) рішень щодо вилучення ЕНІ під час обшуку.

В абз. 4 ч. 2 ст. 168 КПК України встановлено процесуальну процедуру копіювання інформації, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах (далі – інформації, що міститься в ІС), що здійснюється слідчим чи прокурором із залученням спеціаліста. А відповідно до ч. 4 ст. 99 КПК України копії інформації, що міститься в ІС, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа. Таким чином, орган досудового розслідування може забезпечити результативне проведення слідчих (розшукових) дій у частині отримання інформації, що міститься в ІС, як при вилученні електронних носіїв

інформації, так і при виготовленні копії такої інформації в порядку абз. 4 ч. 2 ст. 168 КПК України, що визнається судом як оригінал документа [46, с. 160].

У контексті зазначеного слідчому, прокурору під час проведення обшуку необхідно на основі системного аналізу обстановки на місці проведення слідчої (розшукової) дії обрати процесуально допустимий спосіб отримання інформації – вилучення електронних носіїв інформації або копіювання інформації, що міститься в ІС. Для прийняття зваженого процесуального рішення слідчим, прокурорам пропонуємо використовувати розроблений нами алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку, огляду [46, с. 159-165].

У разі виявлення під час проведення обшуку чи огляду електронних носіїв інформації (знімних (відокремлених) або в складі інформаційних систем) слідчому, прокурору слід установити на місці обставини, які стосуються таких питань:

- Чи потрібен пароль для доступу до електронної інформації? Пароль (значення, ключ тощо) є обов'язковим компонентом системи логічного захисту. Водночас відповідно до абз. 3 ч. 2 ст. 168 КПК України забороняється тимчасове вилучення електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку (далі – ЕІС, КС, МТСЗ), крім випадків, якщо доступ до них пов'язаний з подоланням системи логічного захисту. Тобто виявлення вказаної обставини може бути підставою для вилучення відповідного електронного носія інформації;

- Чи повідомлений пароль для доступу до електронної інформації? Неповідомлення паролів власником, володільцем або утримувачем є формою обмеження доступу до інформації. Це додатковий аргумент на користь прийняття рішення щодо вилучення ЕІС, КС, МТСЗ, бо згідно з абз. 3 ч. 2 ст. 168 КПК України забороняється тимчасове вилучення ЕІС, КС, МТСЗ крім випадків, якщо доступ до них обмежується їх власником, володільцем або утримувачем. Вимогами до паролів, які знімають обмеження в доступі, є їх надання: для адміністративного рівня доступу до електронних даних; до всіх заблокованих віртуальних об'єктів; в явному вигляді або як можливість введення пароля необхідну кількість разів;

- Чи виявлена інформація доказового значення під час проведення експрес-пошуку інформації? У разі виявлення відомостей, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження, електронні носії можна віднести як мінімум до засобів вчинення кримінальних правопорушень. За такої умови згідно з абз. 3 ч. 2 ст. 168 КПК України забороняється тимчасове вилучення ЕІС, КС, МТСЗ, крім випадків, коли такі об'єкти отримані в результаті вчинення кримінального правопорушення чи є засобом або знаряддям його вчинення. Тобто виявлення вказаної обставини може бути підставою для вилучення відповідного електронного носія інформації;

- Чи є необхідність експертного дослідження виявленого електронного носія інформації, інформаційної системи тощо? Згідно з абз. 3 ч. 2 ст. 168 КПК України забороняється тимчасове вилучення ЕІС, КС, МТСЗ, крім випадків, коли їх надання разом з інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження. В окремих випадках необхідно встановити, чи є комп'ютер або телефон засобом створення виявленої інформації доказового значення. Тобто встановлення цієї обставини може бути підставою для вилучення відповідного електронного носія інформації;

- Чи вказані в ухвалі суду електронні носії інформації, інформаційної системи тощо? Відповідно до абз. 2 ч. 2 ст. 168 КПК України тимчасове вилучення ЕІС, КС, МТСЗ для вивчення фізичних властивостей, які мають значення для кримінального провадження, здійснюється лише у разі якщо вони безпосередньо зазначені в ухвалі слідчого судді про дозвіл на обшук (огляд) житла чи іншого володіння особи;

- Чи необхідна копія виявленої інформації для глибокого аналізу? Якщо слідчому, прокурору необхідна копія виявленої інформації, її може бути виготовлено в порядку, визначеному абз. 4 ч. 2 ст. 168 КПК України, що надаватиме такий копії статусу оригіналу документа [46, с. 161–162].

Можливість проведення експрес-пошуку інформації як форми огляду документів під час обшуку, огляду передбачено в ч. 7 ст. 236 КПК України через призму можливості проведення огляду документів, якими є електронні носії інформації. Важливо зауважити, що експрес-пошук не дозволяє проаналізувати

значну частину видалених файлів, а також зашифровані та заблоковані дані, однак така дія надає можливість визначитися з наступними рішеннями при проведенні обшуку, огляду [46, с. 162].

Процесуальна процедура копіювання електронної інформації, що визначена в абз. 4 ч. 2 ст. 168 КПК України (криміналістичне копіювання інформації), є ефективним засобом отримання доказової інформації [455], що може бути надалі дієво використана слідчим та прокурором з огляду на статус такої інформації як оригінала (ч. 4 ст. 99 КПК України). Водночас таке криміналістичне копіювання є технічно насиченим процесом, для реалізації якого потрібна попередня підготовка. Для повноцінного криміналістичного копіювання інформації необхідні спеціальні комп'ютерні програми для обрахування геш-значень та цільовий носій з ємністю, зазвичай не меншою, ніж у носія-джерела. Загалом у даному питанні доцільно керуватися ДСТУ ISO/IEC 27037:2017.

Технічна неможливість копіювання електронної інформації є обґрунтуванням необхідності експертного дослідження. Також у разі неможливості копіювання електронної інформації з об'єктів, що не вказані в ухвалі слідчого судді, слідчий, прокурор може їх тимчасово вилучити в порядку, визначеному ч. 7 ст. 236 КПК України (як речі, що мають важливе значення для кримінального провадження). При цьому у протоколі має бути зафіксовано відомості, що можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження, а метою вилучення – забезпечення збереження цілісності інформації на електронному носії, а не вивчення фізичних властивостей, оскільки такі властивості в достатньому обсязі вивчені до ухвалення рішення про вилучення носія (абз. 2 ч. 2 ст. 168 КПК України).

На нашу думку, застосування запропонованого алгоритму є ефективним інструментом аналізу оперативної обстановки на місці проведення обшуку, огляду в складних процесуальних обставинах та в умовах процесуальної протидії сторони захисту. Алгоритм спрямований на забезпечення послідовного врахування вимог КПК України за досліджуваною проблематикою, ефективне прийняття рішення

слідчим, прокурором щодо вилучення ЕІС, КС, МТСЗ та економію процесуального часу [46, с. 163].

У контексті абз. 3 ч. 2 ст. 168 КПК України набуває важливого значення встановлення змісту таких відомостей, як пароль для доступу до електронної інформації.

Під час кримінального провадження трапляється, що особа, у розпорядженні якої перебуває ЕІС, КС, МТСЗ або доступ до відповідних інформаційних систем, добровільно передає їх органам досудового розслідування. Тобто передаються не лише самі пристрої, але й паролі до таких пристроїв чи акаунти на них, ключі шифрування або доступу до хмарних сервісів. Така поведінка особи може бути зумовлена мотивами співпраці зі слідством з метою пом'якшення процесуальних наслідків. Однак є ризики такої практики: можливість прихованого психологічного примусу, шантажу, або створення обстановки, за якої особа вважає, що не має альтернативи співпраці. Така ситуація ймовірна, коли особу не затримують офіційно, однак створюють становище, що фактично обмежує її свободу пересування або прийняття рішень. Тому факт добровільності передання пристроїв, паролів тощо необхідно належно та детально фіксувати під час слідчої (розшукової) дії.

Утім, добровільне надання особою пристроїв та паролів все ж є «ідеальним» сценарієм під час досудового розслідування. Найчастіше під час проведення обшуку сторона обвинувачення стикається з необхідністю подолання систем логічного захисту (паролів чи шифрування) для отримання доступу до інформації. Правове регулювання подолання логічного захисту під час кримінального провадження в Україні досі залишається недостатньо врегульованим, що створює ризики як для дотримання прав учасників процесу, так і для допустимості отриманих доказів. У зв'язку з цим важливим є огляд ефективних стратегій та технічних засобів подолання систем логічного захисту доступу до сучасних комп'ютерних систем під час кримінального провадження.

Відповідно до ст. 5 Закону України «Про інформацію» можливість захисту інформації є складовою права на інформацію, і тому використання цієї можливості

становить правомірну поведінку, що впливає зі статей 3, 31, 32, 62, 63 Конституції України, ст. 8 Конвенції про захист прав людини і основоположних свобод, ратифікованої Законом України від 17.07.1997 (далі – КЗПЛ). Водночас КПК України передбачає випадки обмеження зазначених конституційних та конвенційних гарантій, зокрема: право слідчого, прокурора долати системи логічного захисту доступу до них, у разі якщо особа, присутня при обшуку, відмовляється їх відкрити чи зняти (деактивувати) систему логічного захисту (абз. 1 ч. 6 ст. 236), вилучати комп'ютерні системи, у тому числі мобільні термінали систем зв'язку, якщо доступ до них пов'язаний із подоланням систем логічного захисту (абз. 3 ч. 2 ст. 168), та можливість арешту комп'ютерних систем чи їх частин у разі якщо доступ до них пов'язаний із подоланням систем логічного захисту доступу (абз. 2 ч. 3 ст. 170) [45, с. 57].

Системи логічного захисту, що обмежують доступ до комп'ютерних систем або їх окремих компонентів, через дію програмних, апаратних або програмно-апаратних механізмів інформаційного захисту ефективно унеможливають для слідчого (прокурора) доступ до інформації, що на них зберігається. Такі засоби найчастіше автоматично вбудовані та застосовуються в смартфонах, планшетах та ноутбуках.

Однак слідчому (прокурору) під час обшуку необхідно встановити наявність відповідної системи. У разі виявлення активної системи логічного захисту доступу слідчому (прокурору) доцільно залучити як спеціаліста (ст. 71 КПК України) фахівців-криміналістів у сфері ІТ для подолання виявлених механізмів захисту інформації.

А. М. Гаркуша (2024) висловлює слушну думку, що на практиці подолання систем логічного захисту доступу часто полягає в потребі встановлення значення пароля, який запитується комп'ютерною системою. Для встановлення значення пароля потрібно отримати доступ до зашифрованих комп'ютерних даних для проведення одного з ефективних силових методів криптоаналізу (силової атаки) – перебирання пароля на основі відомого шифротексту. Наступним завданням є виконання безпосереднього перебирання паролів для визначення дійсного

значення встановленого користувачем пароля. За сприятливих обставин дійсне значення пароля чи ключа шифрування можна отримати з оперативної пам'яті комп'ютерної системи, не вдаючись до перебирання пароля, та застосувати для розшифрування даних. У разі дослідження сучасних смартфонів (планшетів) залучений фахівець-криміналіст також має подолати механізми захисту інформації, які реалізуються вбудованими засобами комп'ютерних систем. З метою копіювання повного чи максимально доступного набору даних має бути реалізована атака, спрямована на отримання доступу до даних, які недоступні штатному користувачу (так зване «отримання вищих привілеїв»), що в сукупності становить окремий етап подолання систем логічного захисту доступу [45, с. 58-59]. Якщо механізми логічного захисту доступу вже подолано або їх не існувало, подальші дії криміналіста зосереджуються безпосередньо на копіюванні даних.

В окремих випадках ефективним може бути використання інвазивних (руйнівних) методів зняття комп'ютерних даних, що полягають у фізичному відокремленні електронного носія інформації через випаювання від комп'ютерної системи та наступному зчитуванні комп'ютерних даних безпосередньо з носія інформації без використання засобів комп'ютерної системи (chip-off) [45, с. 60]. Таким чином, під час проведення обшуку навіть за наявності систем логічного захисту можливо забезпечити здобуття інформації та виготовлення її копії.

Однак виникають ситуації, що потребують прийняття обґрунтованого рішення про необхідність вилучення комп'ютерної системи чи її частин під час проведення обшуку (огляду). Це є лише початковим етапом роботи з відповідним об'єктом, адже від моменту вилучення пристрою виникає потреба у чіткому визначенні його процесуального статусу та подальшого забезпечення цілісності вилученої комп'ютерної системи чи її частин, а також зібраної інформації.

У разі проведення невідкладного обшуку (до постановлення ухвали слідчого судді) вилучені комп'ютерні системи чи її частини отримують статус тимчасово вилученого майна, клопотання слідчого, прокурора про арешт якого, згідно з ч. 5. ст. 171 КПК України, слід подати не пізніше наступного після вилучення робочого дня.

Та навіть у разі проведення планових слідчих (розшукових) дій набуття аналогічного статусу вилученими предметами є доволі частим явищем. Зокрема, у ході підготовки клопотання про проведення обшуку слідчий може припускати, що під час проведення відповідної слідчої (розшукової) дії будуть виявлені комп'ютерні системи чи її частини, що мають значення для кримінального провадження, однак заздалегідь указати в клопотанні їх кількість, характеристики та ідентифікаційні дані зазвичай неможливо. Враховуючи це, такі комп'ютерні системи чи її частини не вказано й в ухвалі слідчого судді про дозвіл на проведення обшуку. Відповідно до ч. 7 ст. 236 КПК України вилучені речі та документи, які не входять до переліку, щодо якого прямо надано дозвіл на відшукання в ухвалі про дозвіл на проведення обшуку, та не належать до предметів, що вилучені законом з обігу, вважаються тимчасово вилученим майном.

Таким чином, комп'ютерні системи чи її частини (технічні пристрої чи електронні носії інформації) у більшості випадків стають тимчасово вилученим майном. Тому виникає у слідчого (а також прокурора) необхідність або подальшого накладення арешту на таке майно, або ж його негайного повернення особі, в якій його було вилучено (ч. 5 ст. 171, ч. 6 ст. 173 КПК України). Відповідно до ч. 9 ст. 170 КПК України у невідкладних випадках і виключно з метою збереження речових доказів або забезпечення можливої конфіскації чи спеціальної конфіскації майна у кримінальному провадженні щодо тяжкого чи особливо тяжкого злочину за рішенням директора НАБУ (або його заступника), директора Бюро економічної безпеки України (або його заступника), погодженим прокурором, може бути накладено попередній арешт на майно або кошти на рахунках фізичних або юридичних осіб у фінансових установах. Такі заходи застосовуються строком до 48 годин, і невідкладно після прийняття такого рішення, але не пізніше ніж протягом 24 годин, прокурор звертається до слідчого судді із клопотанням про арешт майна. Враховуючи зазначене, при роботі з доказами електронної форми така ситуація постає доволі часто.

Важливо зауважити, що абз. 2 ч. 3 ст. 170 КПК України визначає вичерпний перелік підстав для арешт на комп'ютерні системи чи їх частини. При цьому ч. 2

ст. 170 КПК України визначає загальні підстави арешту майна, зокрема, що арешт майна, з огляду на які для накладення арешту на комп'ютерні системи чи їх частини (технічні пристрої, чи ЕНІ) їх потрібно визнати речовим доказом, окрім випадків, передбачених п. 2, п. 3, п. 4 ч. 2 ст. 170 КПК України (пов'язаних з конфіскацією та відшкодуванням шкоди).

Варто акцентувати, що на етапі проведення обшуку процеси здійснення спеціальної конфіскації, конфіскації майна як виду покарання або заходи кримінально-правового характеру щодо юридичної особи та цивільний позов зазвичай ще не ініційовано. Це створює фактично єдиний для слідчого (та прокурора) шлях забезпечити процесуальні вимоги щодо накладення арешту на майно – визнання речовим доказом, безвідносно до процесуальної природи комп'ютерних систем чи їх частин у контексті процесуальних джерел доказів, визначених ст. 84 КПК України.

З моменту вилучення під час обшуку комп'ютерних систем чи їх частин (технічні пристрої, чи ЕНІ) до моменту накладення арешту на це майно (або його повернення власнику) має бути забезпечено належний правовий режим поводження з ним. Клопотання про арешт такого майна повинно бути подано слідчим, прокурором упродовж 48 годин після вилучення майна (ч. 5. ст. 171 КПК України), а ухвала про арешт тимчасово вилученого майна – не пізніше 72 годин із дня знаходження до суду клопотання (ч. 6 ст. 173 КПК України). Тобто комп'ютерні системи чи її частини можуть перебувати в статусі тимчасово вилученого майна до 5 діб.

Відповідно до ч. 4 ст. 168 КПК України після тимчасового вилучення майна уповноважена службова особа зобов'язана забезпечити схоронність такого майна в порядку, встановленому КМУ, а саме Порядку зберігання речових доказів стороною обвинувачення, їх реалізації, технологічного перероблення, знищення, здійснення витрат, пов'язаних з їх зберіганням і пересиланням, схоронності тимчасово вилученого майна під час кримінального провадження, затвердженого постановою КМУ від 19 листопада 2012 р. № 1104.

Після накладення арешту на комп'ютерні системи чи їх частини (технічні пристрої, чи ЕНІ) необхідно: по-перше, розуміти процесуальну природу здобутого доказу, щоб забезпечити належний процесуальним режим роботи, технічну природу здобутих даних, щоб гарантувати їх цілісність та забезпечити належний режим зберігання.

Отже, у разі прийняття рішення про вилучення пристрою правильне визначення його процесуального статусу, своєчасне документування дій та дотримання вимог національного кримінального процесуального законодавства у поєднанні з міжнародними стандартами є ключовими умовами забезпечення цілісності інформації, а отже, допустимості отриманих доказів.

У ході обшуку, як зазначалось попередньо, альтернативою вилучення технічного пристрою чи ЕНІ є копіювання інформації. Тож розглянемо процесуальний режим вилученої під час обшуку копії інформації, носія, на якому вона зберігається, а також забезпечення збереження її цілісності. Виготовлена копія інформації, що міститься в ІС, у разі дотримання вимог ч. 4 ст. 99 КПК України (копія інформації $\times$ (слідчий або прокурор + спеціаліст) = оригінал документа) [125, с. 337], набуває правового статусу документа в розумінні ст. 84 КПК України. Така копія визнається судом як оригінал документа, а не лише як копія в традиційному розумінні. Разом з тим, як уже обґрунтовано в підрозділі 1.4, слід відрізняти логічну копію, яка створюється на рівні файлової системи, від криміналістичної (бітової) копії, яка передбачає повне побітове копіювання всіх даних, включно з видаленими файлами, службовою інформацією та структурою розділів. Обидва типи копіювання мають власні технологічні підходи й передбачають різний рівень технічної складності, що впливає на допустимість результатів, отриманих у ході подальшого аналізу. При цьому особливого значення набуває питання ідентифікації копії, що повинно бути належним чином зафіксовано у протоколі відповідної слідчої дії, зокрема через фіксацію геш-суми скопійованих даних, технічних характеристик носія, на якому міститься копія, а також умов його створення, відповідно до п. 3 ч. 3 ст. 104 КПК України. Фіксація контрольної геш-суми є одним з ключових елементів підтвердження цілісності отриманої інформації

та запобігання сумнівам щодо її модифікації. Також слідчому слід пам'ятати про передбачену ч. 3 ст. 107 КПК України можливість створення резервних копій оригінальних примірників технічних носіїв інформації зафіксованої процесуальної дії та можливість їх зберігання поза матеріалами кримінального провадження.

Ще одним важливим елементом є визначення правового режиму як самої копії, так і ЕНІ, на який вона була зафіксована і де існує. Зазначений фізичний носій, що містить копію, є додатком до протоколу слідчої (розшукової) дії, відповідно до п. 1 та п. 5 ч. 2 ст. 105 КПК України. Особливої уваги заслуговує режим збереження копії після її створення. Відповідно до підходів, закладених у ДСТУ ISO/IEC 27037:2017, такі копії підлягають збереженню з дотриманням вимог цілісності, незмінності та ланцюга збереження (chain of custody). Слідчий має враховувати, що кожен доступ до такого носія має бути задокументований, а фізичний носій — маркований, опломбований та захищений від можливих впливів.

Таким чином, виготовлення копії інформації, що має електронну форму, є не просто технічною процедурою, а важливою складовою процесуальної дії, що потребує гарантування слідчим дотримання вимог кримінального процесуального закону, залучення спеціаліста для забезпечення технічних стандартів, зокрема визначених ДСТУ ISO/IEC 27037:2017 процесів. Копіювання інформації як спосіб отримання доказу електронної форми, актуальний також для огляду, тимчасового доступу до речей і документів, та передбачає аналогічні технічні особливості.

Після обговорення процесуального режиму копій інформації, що мають електронну форму, логічно перейти до ситуацій, коли такі відомості не зберігаються фізично на пристрої, вилученому під час обшуку, а існують у віртуальному середовищі (кіберпросторі). З урахуванням особливостей поширення цифрових слідів у хмарних середовищах, соціальних мережах і web-інтерфейсах актуальності набуває питання ідентифікації, фіксації та належного процесуального закріплення таких джерел інформації. У цих умовах важливим інструментом у роботі слідчого стає Open Source Intelligence (OSINT) — збір розвідувальної інформації з відкритих, легально доступних джерел. У практиці кримінального провадження OSINT виступає як: інструмент оперативної розвідки для

попереднього збору доказової інформації; джерело перевірки версій і гіпотез; спосіб виявлення слідів у кіберпросторі без втручання в обмежений доступ або приватну інформацію.

Аналізуючи норми КПК України, О. О. Торбас вказує, що з урахуванням того, що при OSINT розслідуванні найчастіше використовується інформація, отримана з мережі Інтернет, у кримінальному провадженні вона буде підпадати саме під категорію «документ» [273, с. 102]. З такою думкою вченого варто погодитися. Перевагами OSINT для слідчого є оперативність, доступність і можливість діяти без додаткових дозволів слідчого судді. Однак застосування цієї тактики потребує обов'язкового дотримання вимог КПК України щодо допустимості доказів, їх належного процесуального оформлення, а також оцінки достовірності таких відомостей. Базові положення фіксації інформації з кіберпростору як однієї зі стратегій фіксації доказів електронної форми наведено у підрозділі 2.1.

Вимоги до фіксації інформації з кіберпростору є ще одним важливим елементом OSINT (варто звернутит увагу на роботи таких науковців та практиків як О. В. Дикий та В. В. Сидорчук [72, с. 335], О. В. Бабаєва, Д. В. Авербах, [14, с. 174], О. О. Торбас [273, с. 19–99], Г. М. Горбенко [62, с. 8–189] та ін.), що безпосередньо пов'язаний з процесуальними процедурами.

Найбільшою проблемою використання даних з Інтернету як доказів є складність підтвердження їх автентичності. У зв'язку з цим слідчому необхідно дотримуватися низки вимог. При фіксації електронних слідів з мережі Інтернет доцільно керуватися, як вже зазначалося, Протоколом Берклі [238].

Технічна складність процесів, пов'язаних з доказами електронної форми вимагає ефективних відомчих підходів до підготовки слідчих. Професійна здатність слідчого ефективно працювати з доказами електронної форми залежить не лише від формально закріплених повноважень, а й від рівня його цифрової обізнаності. У чинному законодавстві України відсутні чітко визначені вимоги до технічної компетентності слідчих, що призводить до значної варіативності.

На практиці ефективність поводження з цифровими даними багато в чому залежить від особистої ініціативи конкретного працівника, його технічного досвіду та здатності орієнтуватись у сучасних цифрових середовищах. І це є системною проблемою, оскільки створює ризики втрати, спотворення чи дискредитації доказів електронної форми. У відповідь на ці виклики інституції намагаються компенсувати прогалини за допомогою відомчого навчання та методичних рекомендацій. Зокрема, йдеться про: запровадження відповідних курсів у системі підвищення кваліфікації Міністерства внутрішніх справ України (далі – МВС України) та інших правоохоронних органів, які охоплюють теми логічного копіювання, цифрової ідентифікації, роботи з геш-ідентифікаторами, застосування OSINT-інструментів; проведення спеціалізованих тренінгів для органів досудового розслідування у співпраці з міжнародними партнерами (EUAM, ICITAP, CEPOL), де особлива увага приділяється техніці поводження з інформацією в онлайн-середовищі; формування відомчих протоколів та навчальних алгоритмів; підготовка методичних рекомендацій для органів досудового розслідування.

Дотримання прокурором вимог безпеки під час роботи з електронним сегментом кримінального провадження є невід'ємно складовою загальної системи забезпечення особистої безпеки прокурора та ефективного виконання прокурором службових повноважень. Електронне середовище, як одне з найбільш важливих та найменш вивчених прокурорами потребує особливої уваги та вжиття вичерпних заходів щодо: забезпечення безпеки комп'ютера та службової інформації, що зберігається в електронному вигляді в його модулях пам'яті, забезпечення безпеки засобів автентифікації та авторизації прокурора інформаційних системах та роботи з доказами електронної форми [129, с. 114]

У цьому контексті стає критично необхідним формалізувати вимоги до технічної грамотності слідчих у вигляді чітких стандартів; впровадити обов'язкові міжвідомчі програми навчання на базі академій системи МВС України, СБУ та ін., з уніфікованими підходами; поширювати ефективні практики та алгоритми роботи з доказами електронної форми зокрема завдяки цифровим тренажерам слідчих дій.

Узагальнюючи викладене, можна стверджувати, що ефективна діяльність слідчого при роботі з доказами електронної форми потребує всебічної інтеграції правових, технічних та організаційних механізмів. Тож сформулюємо такі головні вимоги та пропозиції щодо удосконалення практичної роботи: 1) стандартизація процедур: необхідне нормативне закріплення мінімальних вимог до процедур фіксації, копіювання, зберігання та документування обігу доказів електронної форми з урахуванням міжнародних стандартів (зокрема, ДСТУ ISO/IEC 27037:2017); 2) процесуальна уніфікація дій слідчого: чітке розмежування процедур копіювання та вилучення, з обов'язковим фіксуванням геш-ідентифікаторів і параметрів носіїв, забезпеченням chain of custody; 3) удосконалення взаємодії з технічними спеціалістами та експертами: впровадження процедурного регламенту попереднього узгодження технічних дій і меж доступу до інформації, що зменшить ризики порушення принципу пропорційності; 4) розвиток міжвідомчого навчання та підвищення кваліфікації: потреба у створенні системних програм підготовки слідчих та прокурорів щодо роботи з цифровими даними з використанням залученням практичного досвіду та методичних матеріалів; 5) нормативне врегулювання фіксації інформації з відкритих джерел (OSINT): включення до КПК України окремих норм, які б деталізували порядок документування та допустимості таких матеріалів; 6) інституційна підтримка та внутрішні методичні напрацювання: узагальнення практики відомств, розроблення галузевих рекомендацій та інструкцій з огляду на специфіку кіберпростору і транснаціональний характер цифрової інформації.

3.2. Прокурор як суб'єкт роботи з доказами електронної форми в кримінальному провадженні

Прокурор у кримінальному провадженні виконує першорядну роль як представник сторони обвинувачення, забезпечуючи нагляд за додержанням законів під час проведення досудового розслідування у формі процесуального керівництва досудовим розслідуванням та підтримання державного обвинувачення в суді, що охоплює й роботу з доказами електронної форми. Відповідно до пунктів 4–5 ч. 2 ст. 36 КПК України прокурор має право доручати слідчому, органу досудового розслідування проведення у встановлений ним строк слідчих (розшукових) дій, НСРД, інших процесуальних дій або давати вказівки щодо їх проведення чи брати участь у них, а в необхідних випадках – особисто проводити слідчі (розшукові) та процесуальні дії, доручати проведення слідчих (розшукових) дій та НСРД відповідним оперативним підрозділам. Водночас з урахуванням специфіки власної ролі та повноважень прокурор зобов'язаний забезпечити, щоб дії зі збирання, копіювання та передачі доказів електронної форми відповідали критеріям належності, допустимості та достовірності. Прокурор виконує роль координатора між іншими представниками сторони обвинувачення та залученими для роботи з доказами суб'єктами, такими як слідчий, оперативні працівники, спеціаліст або експерт. Крім того, прокурор повинен прогнозувати оцінку доказу судом, враховуючи як національне законодавство (КПК України, закони та підзаконні НПА), так і ратифіковані ВР України міжнародні договори, орієнтири, що визначені міжнародною практикою (ДСТУ ISO/IEC 27037:2017, Протокол Берклі), правові позиції ВС та практику ЄСПЛ.

З огляду на фактично повсюдне проникнення цифрових технологій і наявність доказів досліджуваної категорії чи не в кожному кримінальному провадженні, відповідні знання прокурора у цій сфері важко переоцінити. У цьому розділі акцентуємо увагу на конкретних практичних рішеннях.

Під час досудового розслідування прокурор зобов'язаний здійснити комплексну процесуальну оцінку всіх зібраних доказів, зокрема й тих, що мають

електронну форму, перш ніж приступати до підготовки підозри та обвинувального акта. Особливе значення має їх цілісність, що повинна бути належно підтверджена. Тому варто звернути увагу на окремі аспекти діяльності прокурора щодо гарантування цілісності доказів електронної форми під час досудового розслідування. На відміну від умовно класичних доказів, що мають чітку матеріальну форму і загальні ознаки цілісності у формі фактичної наявності, а також відсутності пошкоджень пакування, питання цілісності доказів електронної форми не настільки очевидне. Зокрема, тут важливим фактором є вразливість електронного носія інформації. Наприклад, навіть фактична наявність доказу та не пошкоджене його пакування не виключає порушення цілісності доказу, можливого внаслідок фізичного впливу або пошкодження логічної структури файлів (умисного чи випадкового). Також в окремих випадках спостерігається деградація носія електронної інформації, що на практиці часто спостерігається для карток пам'яті (розм. «флешка»). Наслідком таких пошкоджень/деградації є неможливість безпосереднього дослідження судом, визнання доказом та постановлення на його основі справедливого судового рішення [109, с. 328].

Враховуючи зазначене, гарантування прокурором цілісності доказів електронної форми набуває принципової ваги. Законодавчо загалом врегульована ця сфера. Відповідно до ч. 2 ст. 100 КПК України сторона кримінального провадження, якій наданий речовий доказ або документ, зобов'язана зберігати їх у стані, придатному для використання у кримінальному провадженні. У контексті сторони обвинувачення, на нашу думку, ці питання є невіддільним аспектом діяльності прокурора як суб'єкта, який реалізує свої повноваження як під час досудового розслідування, так і під час судового розгляду кримінального провадження. Ба більше, діяльність прокурора щодо забезпечення гарантування цілісності доказів електронної форми ефективна саме під час досудового розслідування через призму нагляду за додержанням законів під час проведення досудового розслідування у формі процесуального керівництва досудовим розслідуванням. Зокрема, прийняття прокурором ключових процесуальних рішень щодо погодження повідомлення про підозру та завершення досудового

розслідування (звернення до суду з обвинувальним актом, клопотанням про застосування примусових заходів медичного або виховного характеру) при наявності в провадженні доказів електронної форми необхідно реалізувати з урахуванням необхідності гарантування їх цілісності [109, с. 329].

У цьому аспекті важливим є положення Закону України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» від 15 березня 2022 року № 2137-IX [224, с. 1]. Зокрема, пункт 3 ч. 3 ст. 104 КПК України доповнено абзацом, відповідно до якого прикінцева частина протоколу повинна містити відомості про виготовлені дублікати документів, а також копії інформації, у тому числі комп'ютерних даних, та спосіб їх ідентифікації [155, с. 1]. З урахуванням положень ДСТУ ISO/IEC 27037:2017, належним способом ідентифікації є процедура гешування (обрахування контрольних сум для перевірки цілісності даних) електронних файлів [109, с. 329].

Положення ДСТУ ISO/IEC 27037:2017 детально описують умови, за яких копіювання інформації для використання в юридичних процедурах може вважатися надійним та допустимим з технічної точки зору. Загалом варто виділити дві вимоги: 1) недопустимість унесення змін до первинної інформації, що є об'єктом копіювання, до початку копіювання, під час та після його проведення. Одним з варіантів є підключення ЕНІ до комп'ютера спеціаліста чи слідчого в режимі «тільки читання», наприклад, із використанням пристрою блокування запису; 2) верифікація (перевірка) копії інформації шляхом гешування первинної інформації, копії інформації та порівняння отриманих геш-значень. Це забезпечує можливість математично перевірити та підтвердити цілісність та справжність копії інформації, записаної на цільовий ЕНІ [83, с. 7]. Таким чином, контроль за дотриманням органами досудового розслідування вимог п. 3 ч. 3 ст. 104 КПК України, фіксації геш-значень у протоколах слідчих (розшукових) дій надає прокурору належні та дієві аргументи для підтвердження під час судового розгляду цілісності доказів електронної форми та ефективного використання такого доказу.

Ще один аспект діяльності прокурора щодо гарантування цілісності доказів електронної форми під час досудового розслідування кримінального провадження [129, с. 114] можна сформулювати як уникнення ситуації щодо існування доказу електронної форми, в єдиному екземплярі шляхом виготовлення їх належної копії. Вказане необхідно реалізувати через проведення огляду доказу електронної форми, з виготовленням його «криміналістичної» копії в порядку ч. 4 ст. 99 КПК України (визнаватиметься судом як оригінал документа), з дотриманням вимог п. 3 ч. 3 ст. 104 КПК України та фіксації геш-значень. Це мінімізує ризики втрати доказів електронної форми та гарантує підтвердження їх цілісності [109, с. 330].

З урахуванням зазначеного, перевірка прокурором доказів електронної форми при прийнятті прокурором ключових процесуальних рішень щодо погодження повідомлення про підозру та завершення досудового розслідування (складання та/або погодження обвинувального акта) передбачає необхідність:

- а) перевірити процесуальний аспект, що включає таке: здобуття доказу уповноваженою особою (включено до складу групи слідчих, групи прокурорів, наявність доручення тощо); належна процесуальна підстава, умова або обстановка (наявність відповідного процесуального документа або наступної реалізації належних процесуальних процедур у разі проведення невідкладного обшуку); дотримання встановленої законом процедури (залежно від обставин - відеозапис, поняті, спосіб ідентифікації (гешування) тощо); залучення спеціаліста для забезпечення безпосередньої технічної допомоги, застосування технічних засобів, пояснення процесів, надання консультацій;
- б) перевірити технічний аспект, що включає: наявність електронного носія інформації; належне упакування електронного носія інформації; правильне маркування електронного носія інформації; наявність резервної копії електронного носія інформації (виготовленої в порядку ч. 4 ст. 99 КПК України, що визнаватиметься судом як оригінал документа); перевірка геш-суми даних на електронному носії інформації та збіг геш-сум з тими, що відображені в протоколах слідчих (розшукових) дій [109, с. 330-331].

Для перевірки прокурором наведених вище аспектів пропонуємо розроблений нами бланк технічного документа (див. Додаток И), що допоможе прокурору

оцінити доказ електронної форми під час прийняття ключових процесуальних рішень, за визначеними критеріями, використовуючи позначки для зручності.

Для прокурора надзвичайно важливим є розуміння допустимості й достовірності електронних документів (в розумінні Закону України «Про електронні документи та електронний документообіг») у кримінальному провадженні і як доказів, і як процесуальних документів. Використання електронних документів у їх вузькому розумінні відповідно до Закону України «Про електронні документи та електронний документообіг» у кримінальному провадженні притаманні особливості перевірки та оцінки допустимості й достовірності електронних документів як доказів. Цей спеціальний порядок закріплений та впливає як із КПК України, так і з положень згаданого Закону й іншого регулятивного законодавства [43, с. 73].

КПК України встановлює, що сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, зобов'язані надати суду оригінал документа (ч. 3 ст. 99). Для доказування факту чи обставин, що встановлюються під час кримінального провадження, ч. 3 ст. 99 КПК України передбачає можливість надання суду електронного документа, оригінал якого має таке саме значення, як і документ. КПК України не містить автономного визначення терміна «електронний документ», тому за правилами, установленими ч. 3 ст. 3 КПК України, для визначення цього терміна слід звернутися до спеціальних норм в інших законах України. Відповідно до ч. 1 ст. 5 Закону України «Про електронні документи та електронний документообіг» електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Стаття 7 цього Закону відносить до обов'язкових реквізитів документа електронний підпис або підпис, прирівняний до власноручного підпису відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги», а ч. 3 ст. 6 встановлює, що накладанням електронного підпису та/або електронної печатки завершується створення електронного документа. Згідно з п. 15 ч. 1 ст. 1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» електронний підпис – це

електронні дані, що додаються до інших електронних даних або логічно з ними пов'язуються і використовуються підписувачем як підпис. Перевірка й підтвердження електронного підпису здійснюється з використанням засобів і методів захисту інформації. Саме електронний підпис як обов'язковий реквізит електронного документа дозволяє реалізувати вимогу, встановлену ч. 4 ст. 7 Закону України «Про електронні документи та електронний документообіг» стосовно того, що оригінал електронного документа має змогу довести його цілісність і справжність [43, с. 74].

Погоджуємося з тезою А. М. Гаркуші (2024), що під час досудового розслідування кримінальних правопорушень сторони провадження можуть вільно збирати електронні документи (в розумінні Закону України «Про електронні документи та електронний документообіг») через їх копіювання, а під час судового розгляду – надавати суду їх примірники як докази, при цьому допустимість будь-якого й кожного примірника електронного документа визначається за правилами ч. 3 ст. 99 КПК України як надання оригіналу документа за умови підтвердження електронного підпису. Вимоги до допустимості електронних документів як доказів у кримінальному провадженні різняться залежно від їх походження. Якщо доказом є процесуальний електронний документ, складений стороною обвинувачення під час досудового розслідування кримінального правопорушення, він допустимий у статусі оригіналу документа лише за умови, якщо примірник такого документа підписаний КЕП. Коли ж ідеться про електронні документи, створені іншими особами (не суб'єктами, які ведуть процес) та отримані в результаті збирання доказів (непроцесуальні електронні документи), КПК України щодо цього виду електронних документів не вимагає встановлення виду електронного підпису. Оцінка достовірності електронного документа має включати перевірку та підтвердження електронного підпису, адже останній дозволяє довести як цілісність документа, так і його справжність, установити вірогідне авторство та в окремих випадках гарантовано встановити дату й час створення електронного документа [43, с. 76–77].

Одним із ключових етапів завершення досудового розслідування є відкриття матеріалів кримінального провадження стороні захисту відповідно до ст. 290 КПК України. У контексті доказів електронної форми дана процедура викликає низку практичних і процесуальних питань, пов'язаних з обсягом, способом і формою надання стороні захисту доступу до таких доказів.

У ч. 3 ст. 290 КПК України встановлено обов'язок прокурора (або слідчого за дорученням прокурора) надати стороні захисту доступ та можливість скопіювати або відобразити відповідним чином будь-які речові докази або їх частини, документи або копії з них, а також надати доступ до приміщення або місця, якщо вони знаходяться у володінні або під контролем держави, і прокурор має намір використати відомості, що містяться в них, як докази у суді.

Важливо нагадати, що в підрозділі 1.4 ми вже окреслили підходи щодо розуміння процесуальної природи доказу електронної форми, через призму процесуальних джерел доказів, визначених ст. 84 КПК України. Вказані підходи передбачають розмежування складників доказу досліджуваної категорії як документів та речових доказів. Це має безпосередній вплив на реалізацію процедури відкриття матеріалів кримінального провадження, адже ч. 3 ст. 290 КПК України чітко вказує на «будь-які речові докази або їх частини» та «документи або копії з них». Отже, від розуміння процесуальної природи доказу електронної форми, залежить спосіб реалізації положень ч. 3 ст. 290 КПК України.

Оскільки в досліджуваному нами контексті доказом є саме комп'ютерні дані (електронна інформація, цифровий контент тощо), що в розумінні ст. 84 КПК України є документом, а не фізична оболонка (пристрій), на якому зберігаються дані, що в окремих випадках може бути визнана речовим доказом, то реалізація процесу відкриття матеріалів кримінального провадження має бути здійснена відповідним чином. Тобто прокурор, з огляду на норми ч. 3 ст. 290 КПК України, має законну можливість відкрити стороні захисту всі докази електронної форми як «документи або копії з них». Такі копії мають бути виготовлені з забезпеченням належного підтвердження їх автентичності та цілісності, фіксацією відповідних ідентифікаційних даних та підтверджень у протоколі відповідно до вимог ч. 4 ст.

99 КПК України та положень ДСТУ ISO/IEC 27037:2017. Тобто у разі надання стороні захисту копії інформації це мала б бути криміналістична (побітова) копія (більше див.: підрозд. 1.4) з належною ідентифікацією відомостей (підрозд. 2.2).

Ще на етапі проведення досудового розслідування прокурор має можливість виготовити таку копію, залучивши спеціаліста для проведення огляду усіх електронних носіїв інформації, що є в матеріалах кримінального провадження, та виготовлення їх криміналістичних копій з фіксацією у відповідному протоколі усіх геш-сум комп'ютерних даних.

Така «зведена» копія з усіма комп'ютерними даними може бути також використана як резервна копія для прокурора. До того ж, ця копія залишиться в прокурора після надання всіх доказів суду під час судового розгляду, може зберігатися в матеріалах наглядного провадження та надалі використовуватися групою прокурорів у цьому провадженні для підготовки до судових засідань, підготовки апеляційних чи касаційних скарг тощо. Також у разі пошкодження або знищення наданих суду доказів електронної форми (відповідних носіїв інформації), у прокурора буде копія всіх комп'ютерних даних, що виготовлена відповідно до вимог ч. 4 ст. 99 КПК України та яка визнається судом як оригінал документа.

Наступним аспектом у контексті виконання вимог ст. 290 КПК України є обов'язок прокурора надати стороні захисту «доступ та можливість» скопіювати або відобразити відповідним чином будь-які речові докази або їх частини. Тобто відсутня вимога щодо забезпечення для сторони захисту програмних та технічних засобів або профільного технічного спеціаліста для опрацювання і копіювання цих даних. Так само відсутня вимога щодо надання носіїв з уже скопійованими даними. Всі описані ситуації подекуди мають місце на практиці.

Таким чином, належною процесуальною формою реалізації відкриття матеріалів іншій стороні у частині доказів електронної форми вбачається: створення доступу до криміналістичної (побітової) копії, що відповідає вимогам автентичності й цілісності; забезпечення технічної можливості для сторони захисту скопіювати інформацію — з урахуванням обсягу даних, типу носіїв, рівня захисту (вірусний контроль, обмеження доступу до вихідної інформації тощо); відведення

достатнього часу для ознайомлення та копіювання відповідно до характеру інформації. Тобто фактично прокурор мав би забезпечити електронний носій інформації, на якому зберігаються докази досліджуваної категорії, пристрій апаратного блокування запису (для унеможливлення внесення змін на носій) та кабель з'єднання пристроїв. У разі якщо сторона захисту вимагає від прокурора надання електронних носіїв інформації для копіювання, надання технічного спеціаліста для допомоги у здійсненні копіювання або створення умов для доступу до специфічного ПЗ – прокурору доцільно надати стороні захисту роз'яснення положень ст. 290 КПК України, вказавши, що закон передбачає право на копіювання, але не обов'язок сторони обвинувачення на обслуговування адвоката програмними і технічними засобами або ж технічними спеціалістами, що забезпечуватимуть копіювання доказів. У практичній площині доцільно: фіксувати факт ознайомлення/відмови від копіювання — шляхом залучення понятих, здійснення відеозапису процесу, відображення відповідного запису в протоколі відкриття матеріалів; звернутися до слідчого судді з клопотанням про встановлення строку для ознайомлення з матеріалами — у разі саботажу або зловживання процесуальними правами з боку сторони захисту; документувати відмову сторони захисту від копіювання — і в разі подальших заяв щодо порушення їхніх прав посилатися на зафіксовану поведінку. У сучасній практиці саме такий підхід дозволяє забезпечити ефективне й законне відкриття матеріалів іншій стороні в частині доказів електронної форми без нав'язування обвинуваченню процесуально не передбачених обов'язків і гарантує фіксацію добросовісності дій прокурора в умовах позапроцесуального тиску або зловживань.

Формулювання обвинувачення є ключовим процесуальним актом, що відображає логіку доведення, узагальнення доказів та зв'язок між фактичними обставинами і правовою кваліфікацією діяння. У випадках, коли кримінальне провадження включає докази електронної форми прокурор зобов'язаний приділяти особливу увагу їхній юридичній природі, структурі та процесуальній залученості — належному відображенню встановлених обставин при формулюванні обвинувачення. При формулюванні обвинувачення в тексті обвинувального акта на

основі доказів електронної форми прокурору необхідно виокремити, структурувати та вербалізувати ключові елементи, що мають доказове значення для підтвердження складу кримінального правопорушення, обґрунтовуючи їх посиланням на конкретні цифрові джерела. Метою є не механічне перерахування об'єктів доказування, а логічне поєднання цифрових слідів з юридично значущими обставинами, що розкривають зміст події злочину.

Докази електронної форми можуть бути інтерпретовані не як технічні об'єкти, а як елементи логічної структури події злочину, які в обвинувальному акті відображатимуться через їх зв'язок із суб'єктами, об'єктом посягання, часом, місцем та способом вчинення діяння. Будь-яке представлення у судовому процесі доказів електронної форми має супроводжуватись технічними атрибутами, що забезпечують розуміння судом їх джерела, цілісності та автентичності. Тому прокурор може включати ці дані в реєстрі матеріалів досудового розслідування — із зазначенням геш-сум комп'ютерних даних, що зберігаються на електронних носіях інформації.

Окремого значення набуває підтримання державного обвинувачення під час судового розгляду, де прокурору доцільно: пояснити (за потреби — шляхом залучення спеціаліста для надання консультацій і пояснень) роль доказів електронної форми для підтвердження окремих елементів складу кримінального правопорушення (напр.: «лог-файл підтверджує факт авторизації обвинуваченого за IP-адресою»); забезпечити наочне подання доказу (через трансляцію відеозапису, демонстрацію структури файлу, таблиць метаданих тощо); підтвердити правомірність джерела походження шляхом посилання на процесуальні документи (протоколи, ухвали), додані до протоколів пояснення спеціаліста та висновки експертів тощо.

Ефективне формулювання обвинувачення з урахуванням доказів електронної форми потребує від прокурора не лише технічної обізнаності, а й глибокого розуміння логіки побудови структури обвинувачення. Цифрові сліди повинні бути інтегровані у зміст обвинувального акта як інструменти підтвердження обставин, що мають значення для кримінального провадження, з точним зазначенням їх

джерела, змісту, способу отримання та процесуальної легітимності. Під час судового розгляду прокурору необхідно забезпечити не ізольоване представлення доказів електронної форми а їхню доказову інтеграцію в опис події злочину – як індикатори наміру, механізму вчинення, ролей співучасників чи наслідків діяння. Лише за умови дотримання цих вимог докази досліджуваної категорії можуть виконати свою повну функцію – не лише бути допустимими, а й переконливими в контексті підтримання державного обвинувачення.

Незважаючи на активізацію використання ІТ у кримінальному процесі, практика роботи прокурорів із доказами електронної форми залишається фрагментарною і методично незлагодженою, що й засвідчили результати соціологічного дослідження. Емпіричні дані проведеного опитування (див. Додаток В) засвідчують потребу в системному оновленні підходів до роботи прокурора з доказами електронної форми з урахуванням як загальноновизнаних міжнародних практик (зокрема рекомендацій Протоколу Берклі), так і технічних вимог ДСТУ ISO/IEC 27037:2017. Забезпечення якісної реалізації процесуальних функцій прокурора у цій сфері потребує зміни не лише нормативної, а й освітньої та організаційної парадигми.

Отже, у кримінальному провадженні прокурор відіграє центральну роль у забезпеченні належного збирання, обробки, перевірки, оцінки та представлення доказів електронної форми. Зважаючи на багатоаспектність його повноважень, прокурор зобов'язаний забезпечити дотримання законності та гарантування цілісності доказів досліджуваної категорії на всіх етапах кримінального провадження. Особливу увагу має бути приділено процесуальній та технічній перевірці доказів досліджуваної категорії, зокрема шляхом обчислення та фіксації геш-сум, залучення спеціалістів у сфері цифрової криміналістики, фіксації відповідних обставин у процесуальних документах, дотримання належної процедури відкриття стороні захисту доказів електронної форми, ефективного формулювання та підтримання обвинувачення з урахуванням доказів електронної форми, а також демонстрацію зв'язку між змістом доказу та фактичними обставинами справи.

3.3. Захисник як суб'єкт роботи з доказами електронної форми в кримінальному провадженні

У сучасному кримінальному процесі участь захисника в роботі з доказами електронної форми вимагає активних дій, спрямованих на їх виявлення, отримання, аналіз, оскарження та використання. Докази цієї категорії зазвичай є складними за структурою, обсягом і технічною природою, що зумовлює потребу в додатковій спеціалізованій підготовці захисника, залученні відповідних експертних і технологічних ресурсів.

Актуальність дослідження цієї проблематики пояснюється, по-перше, істотними викликами, що виникають у зв'язку з обмеженим доступом захисника до ЕНІ, що містять докази електронної форми а також відсутністю чіткого процесуального порядку передачі копій таких доказів із належним підтвердженням їх автентичності та цілісності; по-друге, дисбалансом технічних можливостей між стороною обвинувачення і захисту, що проявляється у монополії державних органів на використання деяких інструментів цифрової криміналістики; по-третє, недостатньою нормативною конкретизацією процедур захисту приватності, прав на конфіденційність і персональних даних клієнта у контексті аналізу масивів електронної інформації під час кримінального провадження.

Право сторони захисту самостійно збирати докази, у тому числі й ті, що мають електронну форму, безпосередньо впливає зі змісту ч. 2 ст. 22 та ч. 3 ст. 93 КПК України. Відповідно до останньої норми сторона захисту здійснює збирання доказів шляхом витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових та фізичних осіб речей, копій документів, відомостей, висновків експертів, висновків ревізій, актів перевірок; ініціювання проведення слідчих (розшукових) дій, НСРД та інших процесуальних дій, а також шляхом здійснення інших дій, які здатні забезпечити подання суду належних і допустимих доказів. Ці положення узгоджуються з ч. 1 ст. 20 Закону України «Про адвокатуру та адвокатську діяльність», згідно з якою під час здійснення адвокатської діяльності адвокат має

право, зокрема: звертатися з адвокатськими запитами, у тому числі щодо отримання копій документів, до органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб, підприємств, установ, організацій, громадських об'єднань, а також до фізичних осіб (за згодою таких фізичних осіб) (п. 1); збирати відомості про факти, що можуть бути використані як докази, в установленому законом порядку запитувати, отримувати і вилучати речі, документи, їх копії, ознайомлюватися з ними та опитувати осіб за їх згодою (п. 7); застосовувати технічні засоби, у тому числі для копіювання матеріалів справи, в якій адвокат здійснює захист, представництво або надає інші види правничої допомоги, фіксувати процесуальні дії, в яких він бере участь, а також хід судового засідання в порядку, передбаченому законом (п. 8); одержувати письмові висновки фахівців, експертів з питань, що потребують спеціальних знань (п. 10) [221, с. 1].

А. В. Гутник (Ратнова) (2021) зазначає, що зазвичай під витребуванням науковці розглядають збирання доказів захисником шляхом надсилання адвокатського запиту [240, с. 187].

У сучасному цифровому середовищі захисник може застосовувати такі стратегії збору доказів електронної форми: адвокатський запит до провайдерів телекомунікацій, сервісів хмарного зберігання даних, операторів зв'язку з метою отримання інформації про історію з'єднань, обсяг переданих даних, місцезнаходження пристроїв тощо; ініціювання проведення слідчих (розшукових) дій та НСРД; залучення спеціаліста або технічного консультанта для отримання інформації з ЕНІ (наприклад, аналіз вмісту смартфона клієнта); ініціювання технічного дослідження цифрових артефактів — листування у месенджерах, метаданих фото чи відео файлів, логів систем, резервних копій — для встановлення непричетності особи або штучної природи певної цифрової події.

Важливим аспектом описаної стратегії є використання доказів електронної форми стороною захисту у контексті встановлення алібі або спростування обвинувачення. Йдеться, зокрема, про: резервні копії телефонів або електронної пошти, що підтверджують відсутність певної інформації чи її незмінність; геолокаційні дані з мобільних додатків або хмарних сервісів, що дозволяють

довести фізичне місцеперебування особи під час вчинення інкримінованого кримінального правопорушення; скриншот й технічні звіти про листування у месенджерах (Telegram, WhatsApp, Viber тощо), які можуть довести контекст повідомлень, час їх надсилання та автентичність.

Проте ефективність використання таких даних прямо залежить від дотримання технічних процедур, що забезпечують ланцюг збереження доказів (chain of custody). Такі вимоги полягають у: документуванні дати, часу, способу отримання та збереження копії доказу електронної форми; фіксації контрольної геш-суми цифрових даних до моменту початку аналізу та після копіювання; використанні програмних засобів, що не змінюють структуру даних (наприклад, EnCase, FTK Imager); веденні журналу доступу до цифрової інформації, що використовується стороною захисту як доказ.

Важливе значення для сторони захисту має своєчасне виявлення та належне опрацювання джерел цифрової інформації, що потенційно можуть містити відомості, що виправдовують особу. Результати дослідження M. Burman, O. Smith, O. Brooks-Nay та Y. Brunger (2025) засвідчують, що ефективна діяльність захисника у цій сфері передбачає чітку ідентифікацію відповідних джерел цифрових даних (зокрема повідомлень у соціальних мережах, месенджерах, журналів викликів) [325], визначення їх релевантності та належності до обставин кримінального правопорушення, а також документування усіх етапів їх здобуття та аналізу. При цьому важливим є залучення кваліфікованих технічних спеціалістів з метою забезпечення підтвердження автентичності та цілісності отриманої інформації. Формування клопотань щодо доступу до таких даних має здійснюватися з дотриманням принципів пропорційності й релевантності, з чітким окресленням меж запитуваної інформації та обґрунтуванням її значення для захисту, що мінімізує ризик відмови у їх задоволенні.

Таким чином, збір і подання захисником доказів електронної форми – допустимий, ба більше, необхідний елемент реалізації права на захист. І це вимагає від адвоката не лише правової підготовки, а й базових цифрових компетенцій,

зокрема щодо підтвердження автентичності цифрових слідів, фіксації геш-сум цифрових даних та документування технічної процедури.

Обшук як слідча дія, що безпосередньо пов'язана з виявленням, фіксацією та вилученням доказів електронної форми вимагає від захисника високої тактичної підготовленості. Основою поведінкової моделі захисника у таких випадках є поєднання правових гарантій, визначених у статтях 20, 22, 26, 236 КПК України, із належним захистом адвокатської таємниці, цифрової безпеки й недоторканності технічних пристроїв та ЕНІ, що потенційно містять привілейовану інформацію. Дії адвоката на оглядовій стадії обшуку спрямовані на те, щоб не допустити порушень прав та свобод клієнта та інших осіб, які присутні на обшукуваному об'єкті, захистити їх від можливих необґрунтованих вимог слідчого та інших правоохоронців [161, с. 40].

О. І. Литвинчук, М. С. Сорока, І. В. Колесников та ін. (2020) надають, поміж іншого, рекомендації щодо дій адвоката на попередній стадії обшуку [161, с. 35–36]. Здійснення відеофіксації обшуку є важливим тактичним інструментом, який захисник має право використовувати також як адвокат, відповідно до п. 8 ч. 1 ст. 20 Закону України «Про адвокатуру та адвокатську діяльність» має право застосовувати технічні засоби.

На практиці часом трапляється, що слідчі намагаються залякати захисника, який здійснює відеозапис, тим, що носій інформації (яким, як правило, є смартфон) буде у нього вилучено та долучено до протоколу обшуку, оскільки він є додатком до протоколу слідчої (розшукової) дії й містить доказову інформацію [161, с. 39]. Але захисник повинен наполягати на неприпустимості вилучення його технічних засобів фіксації, якщо такі не є предметом або знаряддям вчинення кримінального правопорушення.

Науковці зазначають, що адвокат одразу має пояснити слідчому, що вилучення його телефону (смартфону) неможливо, оскільки на ньому зберігаються відомості, що становлять адвокатську таємницю. До того ж, примусове вилучення майна адвоката можливе лише під час обшуку житла чи іншого володіння адвоката, дозволу на проведення якого у слідчого зазвичай немає [161, с. 40].

У разі виявлення спроб доступу до пристроїв, на яких потенційно зберігається адвокатська таємниця, захисник може: заявляти під час проведення відповідної слідчої (розшукової) дії про гарантії захисту адвокатської таємниці, передбачені ст. 22 Закону України «Про адвокатуру та адвокатську діяльність», і зафіксувати відповідні факти у зауваженнях до протоколу слідчої (розшукової) дії; вимагати окремої ухвали слідчого судді, яка б легітимізувала такий доступ; ініціювати складання окремого протоколу з переліком потенційно привілейованої інформації, що унеможливило її подальше використання в доказуванні без додаткової санкції; звернутися до Ради адвокатів із зверненням про втручання в адвокатську діяльність через вилучення технічних пристроїв, на яких зберігається адвокатська таємниця.

Крім того, важливо враховувати можливість відображення в Єдиному реєстрі адвокатів України технічних засобів фіксації, якими користується адвокат (мобільні пристрої, камери, накопичувачі). Ця практика ґрунтується на прецедентах неправомірного вилучення комп'ютерної техніки адвоката, що використовувалась виключно для фіксації обшуку [161, с. 40].

Окрему групу тактичних дій складають підстави для відображення зауважень до протоколу обшуку у разі якщо: відсутня деталізація вилучених комп'ютерних систем або їх частин, ЕНІ (їх найменування, тип, ідентифікатори); не зафіксовано процес копіювання або не вказано геш-суми вилученої та скопійованої інформації; втрачено безперервність ланцюга збереження доказу (не задокументовано передача пристрою чи даних).

Такі порушення можуть бути оскаржені у порядку, передбаченому ст. 303 КПК України, а також стати підставою для подання окремого клопотання про визнання недопустимим доказом, з урахуванням стандартів, викладених у ДСТУ ISO/IEC 27037:2017.

Таким чином, ефективна тактика дій захисника при проведенні обшуків, пов'язаних із доказами електронної форми передбачає чітке дотримання нормативних гарантій, активне застосування процесуальних прав, фіксацію

кожного факту порушення, безперервного ланцюга збереження доказів, а також принципову позицію щодо охорони адвокатської таємниці.

На стадії завершення досудового розслідування головне значення для сторони захисту має доступ до матеріалів кримінального провадження, включно з доказами електронної форми. Правовий режим цього етапу визначається положеннями ст. 290 КПК України, згідно з якими сторона обвинувачення зобов'язана надати можливість ознайомитися та відтворити документи, речові докази або їх частини, що планується використати в суді.

Специфіка доказів електронної форми обумовлюється їх процесуальною природою: у більшості випадків комп'ютерні дані (цифровий контент, електронна інформація) відповідно до ст. 84 КПК України є документами, тоді як фізичний носій (пристрій) може набувати статусу речового доказу лише за окремих підстав. Це розмежування безпосередньо впливає на форму доступу, адже сторона обвинувачення має право надати захисту доступ до копії електронної інформації (як документа), що мають бути виготовлені з дотриманням вимог автентичності та цілісності, передбачених ч. 4 ст. 99 КПК України та ДСТУ ISO/IEC 27037:2017.

Разом із тим формулювання ч. 3 ст. 290 КПК України обмежує обов'язки сторони обвинувачення саме наданням доступу до доказів досліджуваної категорії, а також можливістю самостійного копіювання, адже закон не зобов'язує прокурора забезпечувати сторону захисту програмними та технічними засобами або ж спеціалістом, який може таке копіювання здійснити. На практиці це означає, що обсяг і якість відтворення доказів електронної форми значною мірою залежать від власних ресурсів та технічної підготовки сторони захисту.

Таким чином, адвокат, реалізуючи своє право на ознайомлення з доказами електронної форми має враховувати як процесуальні рамки, встановлені ст. 290 КПК України, так і технічні параметри способу їх надання. Від правильного тлумачення цих положень та розуміння технологічних аспектів обробки електронної інформації залежить ефективність використання таких доказів під час судового розгляду кримінального провадження.

Водночас під час відкриття матеріалів кримінального провадження докази електронної форми мають бути надані стороні захисту із належним підтвердженням їх автентичності та цілісності: відображення структури даних, геш-сум, системних логів тощо. У контексті ДСТУ ISO/IEC 27037:2017 важливо враховувати норми, що вимагають забезпечення можливості перевірки автентичності цифрових об'єктів через контрольні ідентифікатори (геш-суми) та *chain of custody*. У зв'язку з цим обґрунтованими є клопотання захисника про надання доступу до доказів електронної форми із зазначенням геш-суми (SHA-256 або інший), метаданих, структурованої інформації журналів доступу, а також супровідної контрольної інформації (середовище отримання, спосіб копіювання, програми перегляду).

Слід зазначити, що вітчизняна правозастосовна практика засвідчує окремі порушення при забезпеченні права сторони захисту на доступ до доказів електронної форми. Типовими є ситуації, коли: матеріали надаються у формі скриншот або конвертованих файлів без метаданих; сторона захисту не допускається до копіювання даних з криміналістичних копій; немає журналів доступу та акти передачі носіїв; ігноруються клопотання про проведення комп'ютерно-технічної експертизи тощо.

Таким чином, право на доступ до доказів електронної форми включає не лише ознайомлення з їх змістом, а й можливість аналізу структури, способу отримання, автентичності та цілісності цифрових даних. З огляду на зазначене, підхід до реалізації ст. 290 КПК України має бути оновлений у практичному вимірі — шляхом закріплення обов'язку сторони обвинувачення надавати доступ до криміналістичної копії ЕНІ (інформації, що міститься в ІС) з забезпеченням належного підтвердження автентичності та цілісності даних.

Варто підкреслити, що докази в електронній формі нерідко містять великі масиви особистої інформації підозрюваного, обвинуваченого, котра не має безпосереднього відношення до предмета доказування у кримінальному провадженні. Тому перед захисником постає критично важливе завдання — забезпечити баланс між доказовою доцільністю та етичними обмеженнями,

пов'язаними із захистом конфіденційних даних. О. І. Гафич (2024) вказує, що адвокат зобов'язаний переконатися, що: були дотримані права на приватність під час отримання доказів електронної форми (наприклад, чи було санкціоновано вилучення приватного листування чи доступ до хмарних сховищ); докази не отримані незаконним шляхом (наприклад, без належної ухвали суду); усі дії слідчих чи оперативних підрозділів були зафіксовані в процесуальних документах (протоколах огляду тощо) [48, с. 342]. Насамперед варто враховувати небезпеку розголошення відомостей про інтимне та особисте життя особи, що не пов'язані з обставинами кримінального правопорушення.

Поділяємо думку дослідників, що адвокату варто пам'ятати, що відповідні відомості (наприклад, логін та пароль) використовуються виключно для цілей контролю захисту даних, резервного копіювання або забезпечення правильної роботи системи обробки даних. Принцип непорушності захисту даних діє й під час досудового розслідування, однак не може використовуватися для прикриття злочину чи правопорушника. Передача цифрової інформації допускається, якщо кримінальний процесуальний закон надає слідчому або прокурору дозвіл на обшук, при цьому право на інформаційну самоідентифікацію особи підпорядковується вимогам правоохоронної системи з обов'язковим дотриманням правил захисту персональної цифрової інформації [161, с. 50–51].

А. В. Скрипник (2021), досліджуючи право на цифрову приватність, робить низку важливих висновків, що варті уваги в досліджуваному контексті, зокрема такі: 1) електронні повідомлення, які були одержані та прочитані адресатом, є інформацією про особисте життя особи (персональними даними про неї) та конфіденційною інформацією; 2) такі повідомлення є об'єктом правової охорони як права на повагу до приватного життя, так і права на таємницю кореспонденції; 3) ознайомлення зі змістом таких повідомлень можливе лише після отримання попереднього судового дозволу, а докази, отримані без такого, мають визнаватися недопустимими; 4) можливими процесуальними шляхами отримання доказів з електронних повідомлень, отриманих та прочитаних адресатом, можуть бути: а) тимчасовий доступ до документів, що містять охоронювану законом таємницю (п.

4 або п. 6 ч. 1 ст. 162 КПК України), із подальшим їхнім оглядом чи проведенням експертизи (відповідає інформаційному аспекту електронних повідомлень); б) огляд таких документів або їх експертиза, які проводяться на підставі судового дозволу як такі, що пов'язані із втручанням у приватне спілкування (ч. 2 ст. 258 КПК України) (відповідає комунікативному аспекту електронних повідомлень) [249, с. 174].

Під час вилучення ЕНІ або ознайомлення з їх вмістом захисник має наполягати на мінімізації обсягу втручання у приватне та сімейне життя свого клієнта. До таких втручань, що потребують обмеження або контрольованого доступу, належать: фотоархіви особистого характеру, що не мають значення для кримінального провадження; інтимне або родинне листування, яке потенційно порушує право на повагу до приватного та сімейного життя, гарантоване ст. 8 КЗПЛ; персональні нотатки або щоденники, що не мають стосунку до предмета доказування.

У разі загрози незаконного використання або розголошення таких матеріалів адвокат може клопотати про їх анонімізацію або псевдонімізацію, відповідно до сучасних цифрових стандартів. Особливо це стосується листування у месенджерах, фотографій, журналів активності користувача, що можуть бути подані в узагальненому або знеособленому вигляді.

Роль захисника полягає не лише у недопущенні вилучення зайвої конфіденційної інформації, а й у документуванні фактів порушення приватності. До засобів такої фіксації належать: зауваження до протоколу обшуку з чіткою вказівкою на те, які саме дані вважаються приватними і вимагають обмеження доступу; відеозапис обшуку, який демонструє відсутність селективності при вилученні пристроїв або масовий доступ до особистих файлів; клопотання про виключення частини інформації зі складу матеріалів досудового розслідування, з обґрунтуванням недопустимості її використання як доказу (у світлі ст. 8 КЗПЛ).

Таким чином, захист конфіденційної інформації в рамках збирання та використання доказів електронної форми є не лише етичним, а й процесуально зумовленим обов'язком. Захисник має забезпечити дотримання цього балансу між

ефективністю слідства і правами особи шляхом використання інструментів правового захисту, технічних засобів контролю, а також своєчасного процесуального реагування на порушення.

Ще одним дуже важливим аспектом є захист конфіденційної інформації самого захисника як адвоката. Особливий режим охорони адвокатської таємниці, як складової права на повагу до приватного життя, закріплений у ст. 8 КЗПЛ. Суттєвий розвиток він отримав у справі «Bersheda та Rybolovlev проти Монако» [327, с. 1]. Обставини справи полягали у тому, що адвокат, діючи в інтересах клієнта, добровільно надала слідчим свій мобільний телефон з метою перевірки автентичності окремого аудіозапису. Попри обмеженість поставленого завдання, слідчий суддя санкціонував вилучення та аналіз усіх даних, що зберігалися на пристрої, включно з видаленими файлами, без належного обґрунтування обсягу та без застосування процесуальних гарантій, покликаних забезпечити збереження професійної таємниці.

Зокрема, ЄСПЛ визнав такі дії порушенням ст. 8 КЗПЛ, наголосивши, що втручання у професійну конфіденційну сферу адвоката можливе лише за наявності «необхідності у демократичному суспільстві» та за умови суворого дотримання процесуальних запобіжників. До таких гарантій ЄСПЛ відніс чітке визначення мети й меж втручання, обмеження обсягу вилучення інформації виключно тими даними, що мають безпосереднє значення для кримінального провадження, та забезпечення незалежного контролю за дотриманням цих меж [327, с. 1].

У рішенні ЄСПЛ також підкреслив, що недотримання цих вимог призводить до надмірного втручання у сферу адвокатської діяльності, підриває довіру між адвокатом і клієнтом та ставить під загрозу ефективність права на захист [327, с. 1]. Фактично, масове копіювання даних з особистого пристрою адвоката, навіть за його початкової згоди, без достатніх правових та технічних обмежень, створює ризик розкриття чутливої інформації, що не має стосунку до предмета розслідування. Ця справа має ключове значення для розуміння стандартів захисту конфіденційної інформації адвоката у цифрову епоху, особливо у контексті опрацювання доказів електронної форми. Вона демонструє, що ефективне

забезпечення адвокатської таємниці вимагає не лише процесуальних приписів на рівні національного законодавства, а й реальних механізмів технічного та організаційного контролю за обсягом і способом втручання у сферу збереження такої інформації.

В умовах кримінального провадження використання доказів електронної форми значною мірою визначається здатністю сторін не лише отримувати, але й самостійно перевіряти їх автентичність та допустимість. Водночас на практиці існує певна технічна асиметрія, коли лише сторона обвинувачення має повний доступ до спеціального криміналістичного обладнання, ПЗ та кваліфікованих експертів, а також виклики верифікації доказів досліджуваної категорії.

Зокрема, слідчі органів досудового розслідування, спеціалісти та експерти серед іншого використовують програмно-апаратні комплекси класу Universal Forensic Extraction Device (UFED) від компанії Cellebrite, які дозволяють: долати системи логічного захисту; створювати повноцінні криміналістичні (побітові) копії; верифікувати цифрові джерела на основі контрольних геш-сум; вилучати інформацію з прихованих секторів або з віддалених даних тощо. При цьому доступ адвокатів до таких програм зазвичай обмежений — як через їх вартість, так і через необхідність спеціальної сертифікації.

Ще однією гострою проблемою є відсутність доступу захисника до криміналістичних (побітових) копій цифрових носіїв, з яких було отримано докази. Автентичність цифрових даних може бути перевірена лише у разі наявності ідентичної бітової копії з контрольними геш-сумами. Якщо така копія не надається стороні захисту, або доступ до неї блокується, унеможливорюється здійснення власного аналізу й повторної перевірки, що прямо суперечить вимогам ст. 290 КПК України.

Крім того, відповідно до проведеного автором Опитування суб'єктів кримінального провадження поширеною є проблема подання доказів у форматах, що не можуть бути прочитані без спеціального ПЗ. До таких належать: звіти *.E01, *.AFF, *.L01 (формати криміналістичних образів); сесійні файли логування з

мобільних пристроїв у форматах SQLite, JSON без структури; резервні копії IOS або Android, що потребують специфічного софту для розшифрування.

За відсутності доступу до такого ПЗ адвокат позбавлений реальної можливості перевірити як сам факт наявності інформації, так і її цілісність. Тому захист має право ініціювати залучення спеціаліста, який би забезпечив декодування, технічну експертизу, надав пояснення або консультації з технічних питань. Доцільність залучення захисником технічного спеціаліста обумовлене: відсутністю у захисника спеціальних знань, технічних та програмних засобів для самостійної обробки цифрових даних; необхідністю підтвердити або спростувати висновок експерта, отримання альтернативної експертизи.

Технічна асиметрія між повноваженнями сторони обвинувачення та сторони захисту у сфері роботи з доказами електронної форми може трактуватися як порушення засади змагальності та висвітлюватися через призму неефективності наявних інструментів захисту. Тому для нейтралізації її відповідних ризиків доцільне таке: процесуальне забезпечення доступу сторони захисту до криміналістичних (побітових) копій ЕНІ; обов'язкове надання стороні захисту інформації, що забезпечує підтвердження автентичності та цілісності доказів електронної форми; розширення практики залучення стороною захисту спеціалістів у справах з великою кількістю доказів електронної форми.

Науковці підкреслюють, що перенесення відповідної цифрової інформації повинно здійснюватися виключно на «стерильні» носії даних, які надалі використовуватимуться для зберігання доказів. Такі носії обов'язково потрібно перевіряти перед використанням, вони повинні бути без шкідливого ПЗ, вірусів, зокрема [161, с. 51].

Захисник, керуючись ст. 93 КПК України, має право самостійно збирати докази або клопотати про надання документів, що підтверджують ланцюг збереження доказів (chain of custody). Також захисник зобов'язаний вжити заходів для ініціювання перевірки автентичності доказів електронної форми й у разі встановлення порушень вжити належних процесуальних заходів щодо подання

клопотання про спотворення доказів та визнання їх допустимими, а також залучення спеціаліста для підтвердження суду фактів підміни чи модифікації.

Особливу увагу захиснику треба звертати на процес передавання технічного пристрою, ЕНІ чи його копії між різними суб'єктами кримінального провадження, адже часто саме на цьому етапі фіксуються прогалини, що можуть викликати сумніви в цілісності даних.

О. І. Литвинчук, М. С. Сорока, І. В. Колесников та ін. (2020) зазначають, що захисникові за допомогою відеозапису та фотозйомки також слід зафіксувати вигляд предметів та документів, які вилучаються, в упакованому вигляді. Крім того, захисник має право: здійснювати фіксацію моменту отримання копії інформації; фіксувати відмову сторони обвинувачення надати відомості, що підтверджують автентичність та цілісність доказів електронної форми а також вносити зауваження до протоколу відкриття матеріалів кримінального провадження в частині відсутності таких відомостей; у разі виявлення невідповідностей вимагати залучення спеціаліста для підтвердження або спростування своїх доводів або ж, за наявності підстав, проведення комп'ютерно-технічної експертизи технічного пристрою чи ЕНІ, вимагати повторного проведення такої експертизи; перевірити факт зазначення у протоколі індивідуальних ознак технічного носія інформації (карти пам'яті, оптичного диска), на якому збережено відеозапис обшуку [161, с. 57-58].

О. І. Гафич (2024) вказує, що докази досліджуваної категорії є вразливими до маніпуляцій, змін або підробки. Через це адвокат повинен: ініціювати перевірку автентичності доказів електронної форми (зокрема, використання геш-сум або інших методів технічного аналізу файлів); за необхідності залучити експертів, які можуть встановити факт змінення або коригування електронного документа; переконатися, що докази не були отримані з мережі чи пристроїв, що викликають сумнів у їхній достовірності [48, с. 342–343].

Зрештою, ефективне реагування захисника на дефекти ланцюга збереження доказів (chain of custody) забезпечує не лише захист прав клієнта, але й формує

правозастосовну практику, спрямовану на стандартизацію практики використання доказів електронної форми в кримінальному процесі України.

Слід зауважити, що участь захисника у кримінальному провадженні, що стосується доказів електронної форми наразі здійснюється в умовах часткової нормативної невизначеності. У чинному КПК України немає норм, які б чітко врегульовували особливості доступу, копіювання, зберігання та аналізу цифрових даних стороною захисту. Це породжує дисбаланс між сторонами процесу. І. П. Андрєєв (2025) пропонує окрему увагу приділити врегулюванню статусу доказів електронної форми отриманих адвокатом, зокрема використанням OSINT-методів у доказовій діяльності, що відповідає сучасним тенденціям цифрової криміналістики [9, с. 105].

Безперечно, специфіка доказів електронної форми вимагає від адвоката високого рівня професіоналізму, цифрової грамотності та здатності швидко адаптуватися до змін у нормативному регулюванні технологічного середовища. Адвокату необхідно володіти як юридичними, так і технічними знаннями, аби забезпечити ефективний захист у таких провадженнях. Уміння працювати з такими доказами, залучати експертів, аналізувати автентичність і допустимість доказів, а також вчасно реагувати на порушення процесуальних норм – це ключові складові ефективної роботи адвоката в умовах цифровізації кримінального процесу та якісного захисту клієнта, як цілком слушно підкреслюють правники [48, с. 343].

Питання стандартизації форматів надання доказів електронної форми є важливим у контексті вдосконалення практики роботи захисника з доказами електронної форми. У цьому контексті варто: закріпити вимоги щодо передачі сторонами кримінального провадження одна одній «читабельних» доказів у відкритих або загальновизнаних форматах (наприклад, E01, PDF/A, CSV); передбачити обов'язок сторін кримінального провадження надавати електронні файли разом з інформацією, що підтверджує автентичність та цілісність даних, зокрема: геш-суми, лог-файли, технічні довідки про обсяг і тип носія тощо;.

У контексті взаємодії із доказами електронної форми особливого значення набуває дотримання адвокатом стандартів професійної етики. Спроби умисної

маніпуляції цифровими слідами, внесення змін до структури даних або використання технологічної необізнаності сторони обвинувачення для викривлення інформації є несумісними з принципами сумлінного здійснення захисту та підривають легітимність самої інституції адвокатури. Саме поведінка захисника повинна стати взірцем етичного балансу між процесуальною активністю та безумовною доброчесністю. Участь адвоката у кримінальному провадженні вимагає не лише професійної компетенції, а й здатності критично оцінювати технічні дані без спотворення фактів та без застосування засобів, що компрометують ідею справедливого судового розгляду. Таким чином, дотримання етичних норм при роботі з доказами електронної форми є важливою гарантією не лише процесуального балансу, а й авторитету адвокатури в цілому.

Підсумовуючи, зазначимо, що діяльність захисника у сфері роботи з доказами електронної форми обумовлює необхідність застосування комплексного підходу, який поєднує процесуальну, технічну та організаційну складові. Ефективна реалізація права на захист у цій сфері передбачає не лише отримання доступу до відповідних даних, але й забезпечення належної ідентифікації, перевірки автентичності та цілісності цифрових даних. Удосконалення процесуальних механізмів доступу, копіювання та дослідження доказів електронної форми у поєднанні з впровадженням уніфікованих технічних стандартів їх обробки є необхідною передумовою забезпечення реальної змагальності та рівності сторін кримінального провадження.

3.4. Суддя та слідчий суддя як суб'єкти роботи з доказами електронної форми в кримінальному провадженні

Під час кримінального провадження суд здійснює низку функцій, пов'язаних із доказами електронної форми на різних етапах — від початкового контролю за дотриманням правових вимог при збиранні таких доказів до остаточної оцінки їх належності, допустимості й достовірності під час судового розгляду.

Слідчий суддя є суб'єктом первинного контролю за дотриманням належної правової процедури при здобутті доказів електронної форми під час досудового розслідування. Він відіграє ключову роль на етапі, коли ще не здійснюється оцінка доказу по суті, але визначаються правові межі його допустимості як результату певної процесуальної дії. Ця роль реалізується через ухвалення рішень щодо проведення обшуку, огляду, накладення арешту на електронні носії інформації або надання тимчасового доступу до комп'ютерних систем або окремих цифрових об'єктів. Такі рішення мають ухвалюватися з урахуванням критеріїв обґрунтованості та пропорційності, що особливо важливо у разі можливого втручання у приватне життя або професійну таємницю. Наявність у структурі доказу метаданих, геш-сум, електронних позначок часу тощо вимагає, щоб суд оцінював не лише юридичну, а й технічну обґрунтованість втручання. Зокрема, клопотання про обшук або арешт комп'ютерної техніки мають містити відомості про зв'язок між ЕНІ та подією кримінального правопорушення, а також вказівки на необхідність створення копій, а не вилучення оригіналів, якщо це не є критично необхідним. Важливим є врахування судом норм ДСТУ ISO/IEC 27037:2017, що стосуються ідентифікації, збирання, фіксації та збереження доказів електронної форми. Функція слідчого судді щодо доказів електронної форми набуває комплексного характеру: поєднання процесуального фільтра, технічної обізнаності, а також механізму первинного гарантування прав сторін.

Повноваження суду під час дослідження доказів електронної форми є комплексним питанням. Під час судового розгляду кримінального провадження суд зобов'язаний забезпечити всебічне, повне й неупереджене дослідження всіх

наданих сторонами доказів. Стосовно доказів електронної форми особливу увагу має бути приділено питанням автентичності, цілісності та достовірності.

Судовий розгляд є центральною стадією кримінального провадження, в межах якої відбувається безпосередня перевірка стороною обвинувачення і стороною захисту фактичних обставин справи та їх правова оцінка. Суддя виконує процесуальну функцію арбітра, однак, на відміну від стадії досудового розслідування, саме тут реалізується повноцінна змагальність та рівність сторін, що безпосередньо впливає на особливості оцінки доказів електронної форми.

З огляду на цифрову природу таких доказів суддя має оцінювати не лише зміст інформації, а й технічні обставини її отримання, зберігання та передачі. Оцінка має враховувати технічні аспекти, які підтверджують автентичність і цілісність доказового матеріалу: геш-суми, журналювання доступу, належність цифрового джерела, дані про час створення або змін, а також відповідність протоколів та звітів вимогам процесуального законодавства. Зокрема, особливу увагу має бути приділено оцінці відповідності процедур зберігання та передачі інформації вимогам, що впливають з принципу збереження ланцюга доказів (chain of custody). Згідно з ч. 1 ст. 94 КПК України суд оцінює кожен доказ з точки зору належності, допустимості, достовірності, а в сукупності — достатності для прийняття процесуального рішення. У випадку з доказами електронної форми додаткове значення набуває технічна обґрунтованість. Суд має брати до уваги, чи може сторона захисту перевірити технічні параметри поданого доказу, чи була забезпечена можливість ознайомлення з копією доказу в форматі, що дозволяє її експертний аналіз, і чи були дотримані вимоги щодо технічного формату, метаданих і можливості відтворення інформації.

Допустимість доказу в кримінальному процесі України є однією з ключових категорій інституту доказування (досліджена в численних дисертаційних дослідженнях [251; 141; 288; 274; 255; 39]) і тісно пов'язана із суворим дотриманням процесуальних приписів на всіх його етапах. Так, відповідно до ч. 1 ст. 86 КПК України доказ визнається допустимим, якщо він отриманий у порядку, встановленому цим Кодексом. Згідно з ч. 1 ст. 87 КПК України недопустимими є

докази, отримані внаслідок істотного порушення прав та свобод людини, гарантованих Конституцією та законами України, міжнародними договорами, згода на обов'язковість яких надана ВР України, а також будь-які інші докази, здобуті завдяки інформації, отриманій внаслідок істотного порушення прав та свобод людини. Фактично, допустимість доказу є процесуальним визнанням його придатності до використання у доказуванні, що передбачає дотримання вимог законності під час його пошуку, фіксації та використання. Йдеться, зокрема, про дотримання прав і свобод людини, правомірність проведення слідчих (розшукових) дій тощо. У своїй сукупності ці елементи спрямовані на забезпечення прав і свобод учасників кримінального провадження, створення процесуальних гарантій, що дозволяють вважати отриману інформацію такою, що заслуговує на довіру з боку суду.

Зокрема, правила оцінювання доказу електронної форми, на предмет його допустимості наведено в постанові об'єднаної палати Касаційного кримінального суду (далі – ККС) ВС від 29.03.2021 у справі №554/5090/16-к [87].

Суддя також має розглядати клопотання сторони захисту про визнання доказів недопустимими. Така оцінка вимагає техніко-правової аргументації та здатності судді критично сприймати матеріали з цифрових джерел, з огляду на те, що навіть незначні розбіжності можуть бути проявом маніпуляції або зміни доказу.

Враховуючи зазначене, доцільно виокремити деякі категорії доказів електронної форми та визначити ключові характеристики, які суд має враховувати при їх оцінці. Такий підхід дозволяє уніфікувати судову практику, підвищити якість дослідження цифрових даних та забезпечити дотримання принципу допустимості доказів відповідно до вимог кримінального процесуального законодавства України. Якщо до суду подається оригінальний технічний пристрій (смартфон, ноутбук, планшет, зовнішній носій інформації, сервер, маршрутизатор тощо) суд зобов'язаний перевірити дотримання цілісності та автентичності інформації, а також відсутність стороннього втручання. Необхідне належне встановлення ідентифікаційних ознак об'єкта — серійного номера, моделі пристрою, MAC-адреси чи інших унікальних ідентифікаторів. Окремо слід

з'ясувати, чи проведено фіксацію інформації відповідно до вимог ДСТУ ISO/IEC 27037:2017, що має істотне значення для підтвердження достовірності доказу.

Під час дослідження судом копій інформації з комп'ютерних систем чи ЕНІ особливе значення має розмежування звичайних копій від криміналістичних (побітових) копій. Звичайна копія є лише відтворенням файлів або каталогів, що можуть зазнати змін у процесі копіювання, тоді як криміналістична копія забезпечує бітове відтворення усього вмісту носія, включно з вільними секторами та метаданими. Вимога підтвердження тотожності таких копій з оригіналом та їх цілісності передбачає обов'язкову фіксацію геш-значень (геш-сум) під час створення криміналістичної копії, що мають бути зазначені у протоколі слідчої (розшукової) дії та повторно перевірені під час дослідження доказу в суді. Збіг геш-сум, зафіксований на обох етапах, підтверджує цілісність інформації. Копії інформації (як документи), отримані у порядку ч. 4 ст. 99 КПК України (слідчий або прокурор + спеціаліст), визнаються у суді оригіналом документа. Таким чином, надання саме криміналістичної копії з належним документуванням процедури її створення, фіксацією і перевіркою геш-сум, а також дотриманням вимог ч. 4 ст. 99 КПК України забезпечує процесуальну допустимість таких матеріалів.

Під час оцінки доказів електронної форми суд повинен виходити з того, що відсутність належного технічного підтвердження їх автентичності і цілісності унеможливорює їх безумовне визнання допустимими. Суду слід перевіряти наявність геш-сум, зафіксованих у протоколах слідчих (розшукових) дій, а також їх збіг під час дослідження доказу. Виявлення невідповідностей, відсутності геш-сум або логів, брак інших належних ідентифікаційних даних варто оцінювати критично. З метою усунення сумнівів у автентичності, цілісності та достовірності таких доказів суд може залучити спеціаліста, який надасть фахові пояснення щодо технічних аспектів функціонування та обробки даних, або, за потреби, також призначити комп'ютерно-технічну експертизу для отримання об'єктивних висновків щодо внесення змін до цифрової інформації, наявності ознак втручання чи модифікації.

Оцінка доказів електронної форми та отримані з відкритих джерел (публічні вебресурси, соціальні мережі, відеогостинги чи інші відкриті бази даних) потребує уніфікованого підходу, який враховує специфіку їх походження та технічні параметри. Ключовими аспектами для суду є встановлення автентичності, відтворюваності та достовірності такої інформації. У цьому контексті варто врахувати положення Протоколу Берклі як методологічної основи для фіксації відомостей з відкритих джерел. Він визначає вимоги щодо послідовного документування процесу збору інформації, збереження метаданих та забезпечення можливості незалежної перевірки отриманих результатів. Суддям слід ураховувати, що з огляду на динамічний характер онлайн-ресурсів, своєчасність фіксації та правильне технічне відтворення змісту мають вирішальне значення. У разі виникнення сумнівів щодо технічних аспектів отримання чи відтворення даних доцільним є залучення спеціаліста у сфері OSINT, який надасть фахові пояснення.

Досліджуючи докази електронної форми отримані у порядку міжнародної правової допомоги, суд зобов'язаний перевірити дотримання процедур, передбачених міжнародними договорами України та нормами національного кримінального процесуального законодавства. Важливим є розуміння того, що такі матеріали мають бути отримані саме за результатами надання міжнародної правової допомоги, визначеної КПК України, а не лише через оперативні канали взаємодії, як-от мережа SIENA або подібні інформаційні системи. Звернення до національного контактного пункту, що забезпечує цілодобову взаємодію з іншими державами в межах процедур Конвенції про кіберзлочинність (далі – НКП 24/7), не може замінювати передбачену КПК України процедуру, якщо йдеться про докази, призначені для використання в судовому розгляді. При цьому суд повинен встановити законність джерела та способу отримання таких доказів, наявність підтвердження компетентного органу іноземної держави, а також дотримання вимог щодо цілісності цифрової інформації (гешування, ведення журналів доступу, збереження ланцюга збереження даних).

При дослідженні судом доказів електронної форми та є електронними документами в розумінні Закону України «Про електронні документи та

електронний документообіг», суд зобов'язаний перевіряти їхню автентичність відповідно до вимог цього Закону. Основними елементами такої перевірки є наявність електронного підпису, встановлення наявності та відповідності електронної позначки часу, що у сукупності підтверджують авторство документа, його незмінність з моменту підписання та час створення. Для електронних процесуальних документів застосування саме КЕП, а не звичайного електронного підпису, є обов'язковим (див. підрозділ 1.4 та 2.2).

Отже, під час судового розгляду суд виконує роль не пасивного спостерігача за доказами, що їх надали сторони, а активного суб'єкта контролю за їх автентичністю та цілісністю, а отже й допустимістю.

Особливості дослідження доказів електронної форми в судовому розгляді вимагають чіткого дотримання процесуальної послідовності дій та, за потреби, залучення спеціальних суб'єктів, таких як спеціаліст, експерт та суд.

Процес дослідження доказу електронної форми, під час судового розгляду поділяється на три основні етапи: 1) підключення носія — на цьому етапі слід забезпечити фізичний доступ до цифрового пристрою та його підключення з дотриманням вимог щодо захисту даних від внесення в них змін. Участь спеціаліста, відповідно до ст. 360 КПК України, забезпечує роз'яснення сторонам призначення ПЗ, особливостей функціонування апаратної частини та термінології; 2) перехід до місця зберігання файлу — технічне розмежування цього етапу спрямоване на локалізацію інформації в цифровому середовищі. Тут важливо зафіксувати дії осіб, що здійснюють навігацію по пристрою, забезпечити відеозапис екрана, ідентифікацію шляхів доступу до інформації; 3) презентація і дослідження доказу — фінальна стадія передбачає візуалізацію цифрових слідів (файли, листування, медіа тощо), їх дослідження, тлумачення та оцінку.

Для забезпечення дієвості наведеного алгоритму суду варто орієнтувати сторони кримінального провадження на завчасне подання структурованих навігаційних реквізитів до кожного доказу електронної форми. Такі реквізити повинні забезпечувати безпомилкову локалізацію релевантного фрагмента у цифровому середовищі та його відтворюваність: повний шлях на носії (ієрархія

каталогів і назва файлу), ідентифікатори елементів листування, посилання на метадані, часові позначки або діапазони для аудіо- та відеозаписів, вказівки на сторінки й точні місця в текстах, зазначення програмного та апаратного середовища доступу. Ефективним у досліджуваному контексті є також чітка кореляція між елементами предмета доказування та конкретним фрагментом відповідного доказу електронної форми, розкриваючи місце зберігання інформації на ЕНІ та конкретні фрагменти. Такий спосіб подання доводів забезпечує суду можливість здійснити безпосереднє й повне дослідження електронної інформації, коректно відобразити встановлений причинно-наслідковий зв'язок у мотивувальній частині рішення та, у разі потреби, належним чином застосувати процесуальні інструменти (визначення порядку дослідження, залучення спеціаліста чи експерта). У підсумку підвищується обґрунтованість вироку або ухвали, а оцінка доказів здійснюється відповідно до вимог змагальності, безпосередності та внутрішнього переконання суду, сформованого на підставі всебічного, повного й об'єктивного дослідження.

При дослідженні доказів електронної форми під час судового розгляду ключовим є своєчасне застосування процесуальних механізмів, що забезпечують належну оцінку, перевірку та дослідження таких доказів. У цьому контексті положення статей 332, 333, 356, 360 КПК України можуть бути застосовані судом залежно від складності технічної природи цифрових об'єктів доказування.

Згідно зі ст. 333 КПК України під час судового розгляду можливе здійснення тимчасового доступу до речей і документів, якщо одна зі сторін клопоче про дослідження відомостей, які мають значення для встановлення істини у справі, але з різних причин не були отримані на досудовому етапі. Ідеться, зокрема, про випадки, коли: під час судового розгляду встановлено факт існування технічних пристроїв, ЕНІ або облікових записів, що пов'язані з предметом доказування, але які не здобуті під час досудового розслідування; стороні захисту стало відомо про існування альтернативних цифрових джерел (наприклад, резервних копій, логів, геолокаційних даних); з метою підтвердження автентичності чи обґрунтування недопустимості наданого доказу виявлена потреба у витребуванні додаткової

інформації від оператора телекомунікації, з хмарного сховища, зовнішнього сервера тощо.

У разі виникнення обґрунтованих сумнівів щодо цілісності або достовірності доказу електронної форми, керуючись ст. 332 КПК України, суд має повноваження постановити ухвалу про проведення судової комп'ютерно-технічної експертизи. Така необхідність може виникнути, зокрема: якщо сторона кримінального провадження заявила про підробку досліджуваного доказу, втручання або маніпуляцію з боку іншої сторони кримінального провадження; якщо бракує належних ідентифікаційних даних досліджуваної цифрової інформації, таких як геш-суми, журнали доступу, протоколи копіювання; у разі виявлення суперечностей між технічними аспектами досліджуваних доказів, відображених у протоколах слідчих дій, та встановленими під час судового розгляду фактичними технічними даними.

Положення ст. 356 КПК України надають можливість допитати експерта в судовому засіданні. Такий допит доцільний у разі необхідності: перевірки правильності застосованих методик дослідження доказу електронної форми, використаних під час проведення судової комп'ютерно-технічної експертизи; аналізу питань достовірності, автентичності та цілісності інформації, що досліджувалася під час проведення експертизи; підтвердження або спростування можливих фальсифікацій, модифікацій або відсутності належного технічного контролю при збиранні чи передачі доказу для проведення експертизи; з'ясування кваліфікаційних характеристик експерта, рівня достатності вихідних відомостей, а також обґрунтованості застосованих ним підходів до фактів.

Нормами ст. 360 КПК України передбачена можливість залучення спеціаліста для надання суду консультацій і роз'яснень. Йдеться про особу, яка володіє спеціальними знаннями в галузі ІТ, цифрової безпеки, комп'ютерної криміналістики, а також інших суміжних сфер, і здатна надати фахову оцінку щодо: особливостей функціонування програмно-апаратного середовища носія, що досліджується (наприклад, серверної структури, системних налаштувань, конфігурацій безпеки); специфіки технічних форматів, алгоритмів гешування,

шифрування, зберігання та резервного копіювання даних; інтерпретації цифрових артефактів: лог-файлів, журналів подій, метаданих, облікових записів тощо; з'ясування змісту та значення технічної термінології для правильного сприйняття доказу судом.

Таким чином, зазначені положення КПК України становлять процесуальну основу належного реагування суду на виклики, що виникають під час аналізу технічно складних, верифікаційно чутливих об'єктів доказування. Застосування статей 332, 333, 356 та 360 КПК України дозволяє забезпечити повноцінне дослідження доказів електронної форми відповідно принципів кримінального процесу та стандартів цифрової криміналістики.

У процесі дослідження доказів електронної форми особливу увагу варто приділяти вибору джерела, котре підлягає аналізу в судовому провадженні. З огляду на сучасні технічні стандарти, зокрема положення ДСТУ ISO/IEC 27037:2017, пріоритетною є криміналістична (побітова) копія інформації, створена у суворій відповідності до процедур ідентифікації, вилучення, фіксації та збереження цифрових слідів.

Дослідження оригінального пристрою, особливо коли мова йде про мобільні телефони, пов'язане із високим ризиком незворотних змін у системній структурі даних. Увімкнення смартфона чи іншої комп'ютерної системи призводить до автоматичного запуску програмних процесів (ініціалізація ОС, оновлення системних логів, фонове підключення до мережі тощо), що змінює вміст пам'яті пристрою, включаючи часові мітки, лог-файли, кеш-записи та інші метадані. Таким чином, будь-яке втручання в оригінал фактично знищує стан цифрового сліду, який існував на момент вилучення відповідного доказу.

Порушення цілісності проявляється, зокрема, у розбіжності геш-сум між первинним криміналістичним образом (якщо він створений під час або відразу після вилучення) та пристроєм після дослідження або простого увімкнення. У цифровому вимірі це означає, що єдиним достовірним джерелом доказової інформації залишається саме побітова копія, яка не змінювалася з моменту

створення, а тому здатна слугувати об'єктом як для аналізу сторін, так і для призначення комп'ютерно-технічної експертизи.

На практиці типовою є ситуація, коли сторона захисту ставить під сумнів автентичність доказів електронної форми заявляючи про втручання до пристрою під час слідчих (розшукових) дій. Це є поширеною стратегією захисту, особливо у справах, де ключовим джерелом даних є саме мобільний пристрій. У разі якщо було втрачено первинний стан такого носія, призначення об'єктивної експертизи стає неможливим, а отже, і доказ втрачає свою юридичну придатність. Саме тому комп'ютерно-технічна експертиза завжди проводиться не шляхом вивчення даних на оригінальному пристрої, а на його криміналістичній (побітовій) копії, створеній експертом під час проведення експертного дослідження з використанням сертифікованого ПЗ. Експерт фіксує геш-суму носія перед копіюванням, формує криміналістичну (побітову) копію — з повним відображенням усіх службових і користувацьких структур — і вже з нею проводить необхідні дії й обчислення.

У цьому контексті слід також проаналізувати вимоги кримінального процесуального законодавства щодо дослідження оригіналів доказів. Хоча ст. 23 КПК України передбачає безпосередність дослідження доказів судом, у випадку доказів електронної форми копія інформації, що виготовлена відповідно до вимог ч. 4 ст. 99 КПК України, визнаються судом як оригінал документа, а криміналістична (побітова) копія ЕНІ, що виготовлена відповідно до норм ДСТУ ISO/IEC 27037:2017, з технічної точки зору, є тотожною, за умови повного збігу геш-сум. Геш-сума забезпечує математичне підтвердження цілісності копії, тому з технічної точки зору така копія визнається рівноцінною оригіналу, а часом — навіть пріоритетною, якщо наявне порушення первинного стану пристрою при його увімкненні й дослідженні недалекоглядними суб'єктами кримінального провадження.

Таким чином, досліджуючи докази електронної форми суд зобов'язаний враховувати технічну специфіку поводження з технічними пристроями та ЕНІ і надавати перевагу дослідженню саме криміналістичної копії, за умови її належного

створення, фіксації й підтвердження цілісності відповідно до міжнародних і національних стандартів.

Роль для суду спеціаліста (у сфері ІТ) під час судового розгляду кримінального провадження важко переоцінити. Дослідження доказів електронної форми нерозривно пов'язане з технічними аспектами, які можуть бути складними для сприйняття осіб без спеціальних знань. У таких випадках істотну роль відіграє залучення спеціаліста у сфері ІТ, передбачене ст. 71 КПК України. За клопотанням сторін кримінального провадження або за власною ініціативою суду спеціаліст може бути залучений для пояснення технічних обставин, що мають значення для оцінки доказів, зокрема відповідно до ч. 7 ст. 332 КПК України.

Основна функція технічного спеціаліста у судовому розгляді полягає у роз'ясненні суду, а також учасникам процесу, особливостей структури, формату, джерела та шляху проходження електронних даних. У контексті оцінки доказів електронної форми спеціаліст може надання роз'яснень щодо: особливостей функціонування комп'ютерних систем чи їх частин; різниці між оригіналом і копією (криміналістичною (побітовою) чи логічною); значення геш-функцій як способу верифікації цілісності; технічного значення журналів доступу (логів); алгоритмів шифрування, формування метаданих, часових міток тощо.

Залучення спеціаліста дозволяє унеможливити формалізований підхід до оцінки цифрових об'єктів — натомість сприяє вивченню глибших контекстуальних обставин щодо достовірності та автентичності та цілісності даних. Це особливо важливо в умовах, коли сторони надають різні тлумачення одного й того ж цифрового об'єкта — наприклад, щодо правдивості вмісту чатів або відповідності скриншот первинному джерелу.

Не менш значущою є роль спеціаліста у вирішенні питання про потребу у проведенні судової експертизи. За результатами наданих пояснень суд може дійти висновку про необхідність призначення експертного дослідження. У зв'язку з високим рівнем технічної складності доказів електронної форми залучення спеціаліста не повинно сприйматись як виняток. Це — необхідний компонент, що дозволяє суду ухвалити об'єктивне, зважене рішення на основі комплексного

розуміння як юридичних, так і технічних обставин справи. При цьому участь спеціаліста має бути процесуально фіксованою: його пояснення мають вноситись до протоколу, з правом сторін поставити уточнювальні запитання. Суддям важливо зрозуміти, що роль спеціаліста — не в тому, щоб замінити собою суд або експерта, а в тому, щоб зробити складне — зрозумілим.

Ефективне здійснення судочинства в умовах стрімкої цифровізації кримінального процесу вимагає не лише зміни нормативного підходу до доказів електронної форми а й оновлення матеріально-технічного та організаційного забезпечення діяльності суду. Актуальність цієї проблематики пов'язана з практичною неспроможністю низки судів забезпечити належне дослідження цифрових об'єктів, особливо у справах, де їх обсяг або структура виходять за межі традиційного доказового масиву.

Однією з ключових проблем залишається відсутність базових засобів візуалізації електронних матеріалів у залах судових засідань. Більшість судів не обладнано мультимедійними проєкційними системами, що унеможливорює ефективну демонстрацію цифрових об'єктів. Такі матеріали часто потребують точного масштабування, коректної передачі даних, збереження шрифтів, кольорової гами тощо — чого не можна досягти без спеціалізованого ПЗ або професійної демонстраційної техніки.

Не менш гостро постає питання доступу до цифрових пристроїв безпосередньо в судовому засіданні. У багатьох випадках суд не має технічної можливості оперативно перевірити наданий стороною носій — зокрема у форматах, що потребують встановлення ліцензійного ПЗ. Така ситуація призводить до знецінення змісту доказу або його поверхового сприйняття.

Організаційно відсутня і процедура захисту доказів електронної форми від спотворення під час відтворення. Наприклад, демонстрація відеофайлу з камер спостереження або експортованого листування з месенджера в PDF-форматі без підтвердження відповідності геш-сум або лог-файлів унеможливорює оцінку його автентичності та цілісності. Часто на практиці мають місце випадки, коли одна сторона демонструє копію скріншоту з відкритого браузера без підтвердження

джерела, часу створення або метаданих, що є неприйнятним з позиції доказової цінності.

В окремих кримінальних провадженнях сторони, аби забезпечити повноцінне сприйняття складного цифрового об'єкта, змушені самотійно залучати спеціаліста з технічною підтримкою (ноутбук, ПЗ, кабель для проєктора), при цьому не маючи жодної впевненості у наявності базових умов у залі суду — відповідного екрана, джерела живлення, стабільного доступу до мережі.

Таким чином, судова система повинна бути інституційно готовою до роботи з доказами електронної форми шляхом створення технічно забезпечених середовищ розгляду справ — із гарантованим доступом до технічних пристроїв, ПЗ, інструментів візуалізації, а також підготовленого персоналу, здатного забезпечити проведення дослідження.

Фахова підготовка суддів до роботи з доказами електронної форми є важливим аспектом ефективної роботи. Суд під час судового розгляду кримінального провадження виконує ключову функцію верифікації доказів електронної форми оцінюючи не лише їх зміст, а й процедуру отримання, умови фіксації, збереження та подання в суд. У сучасному кримінальному процесі така роль вимагає постійного оновлення знань, зокрема з технічних аспектів обробки цифрової інформації, а також вміння інтерпретувати та застосовувати профільні міжнародні стандарти.

З огляду на стрімку цифровізацію кримінального процесу та поширення доказів електронної форми критично важливим стає питання належного рівня професійної підготовки суддів. Ця компетентність включає не лише правове, а й технічне розуміння процесів створення, обробки, збереження та дослідження доказів електронної форми.

Згідно з результатами проведеного нами Опитування суб'єктів кримінального провадження, переважна більшість суддів визнали труднощі у самотійному аналізі доказів електронної форми через обмежені знання щодо технічних аспектів їх походження та структури, що є закономірним з огляду на складність сучасних ІТ. Серед виявлених проблем фігурують: нерозуміння

принципів гешування, складнощі розуміння значення метаданих, проблеми з ідентифікацією копії та оригіналу електронного об'єкта, відсутність досвіду аналізу лог-файлів або форматів з обмеженим доступом. Це свідчить про необхідність розширення відповідних тематик у системі підвищення кваліфікації суддів.

Національна школа суддів України системно працює над удосконаленням цифрової грамотності суддів шляхом реалізації програм підвищення кваліфікації. Так, впродовж 2019–2023 рр. у межах навчальних модулів було запроваджено спеціалізовані курси, присвячені роботі з електронними носіями інформації, методам аналізу доказів електронної форми. Серед рекомендованих до вивчення матеріалів, активно застосовуваних під час тренінгових занять, заслуговує на увагу збірник навчальних матеріалів тренінгу для суддів «Застосування електронних доказів під час розгляду справ, пов'язаних з корупцією» (2019, розробники С. Браун, В. С. Овсянніков, С. В. Шинкоренко) [25], що містить цікаві матеріали щодо технічної природи доказів електронної форми серед яких: принципи функціонування мережі Інтернет, використання телефону як доказу, можливості цифрової криміналістики, способи виявлення прихованих файлів, технічні та юридичні особливості криптовалюти тощо.

Окрім внутрішньовідомчої підготовки, позитивною практикою є проведення міждисциплінарних семінарів за участю ІТ-спеціалістів. Такі заходи дозволяють підвищити рівень технічної обізнаності суддів, сформувані у них розуміння основних понять, зокрема принципу «chain of custody», процедур гешування, структури цифрових слідів, алгоритмів шифрування, розмежування первинних і вторинних джерел цифрової інформації. Водночас суддя ККС ВС Надія Стефанів наголошує, що самі судді відповідають за підвищення власних професійних знань стосовно використання електронних доказів. «Суддя сам має дбати про те, щоб бути в курсі всіх останніх новин щодо документів і стандартів та застосовувати їх відповідно до чинного процесуального законодавства» [257, с. 1].

У контексті зазначеної перспективи вбачається включення до обов'язкової програми підготовки суддів таких навчальних блоків, як: функціонування

глобальної мережі Інтернет, принципи верифікації цифрових об'єктів, основи блокчейн-технологій, а також розділів, присвячених ДСТУ ISO/IEC 27037:2017, Протоколу Берклі, Конвенції про кіберзлочинність. Знання цих нормативів та принципів дозволить судді всебічно оцінювати допустимість доказу та гарантувати дотримання процесуальних стандартів при розгляді справ з цифровим елементом.

Таким чином, належна оцінка судом доказів електронної форми прямо залежить від належного рівня підготовки суддів, що потребує подальшого розвитку системи підвищення кваліфікації з урахуванням міждисциплінарних підходів та міжнародного досвіду.

Окреслення процесуальної ролі судді, а також організаційних і навчальних передумов для забезпечення належної оцінки суддею доказів електронної форми дозволяє сформулювати цілісне уявлення про механізми реалізації принципів кримінального процесу в умовах цифрової трансформації кримінального провадження. Водночас саме правозастосовна практика ВС становить важливий емпіричний фундамент для оцінки ефективності цих механізмів.

Г. Авдєєва, Е. Живуцька-Козловська (2023) вказують, що суди кримінальної юрисдикції України іноді ухвалюють протилежні рішення щодо визнання цифрової інформації допустимим доказом за тих самих умов. Причини невизнання судом допустимими доказами цифрової інформації: надання суду копії цифрової інформації, а не оригіналу; проведення НСРД та отримання цифрової інформації без доручення на те слідчого, прокурора й без ухвали слідчого судді; невідкриття стороні захисту доручення на проведення НСРД; відсутність процесуального оформлення рішення слідчого або прокурора про залучення до проведення НСРД «іншої особи» та ін. [4, с. 141].

З огляду на зазначене, логічним продовженням аналізу є розгляд актуальної судової практики ВС, в якій сформульовані підходи до оцінки та використання доказів електронної форми під час кримінального провадження. Попри актуальність вказаного питання, усталена судовою практикою сформована лише в частині оцінки окремих видів доказів.

Зокрема, правила оцінювання доказу електронної форми, на предмет його допустимості наведено в постанові об'єднаної палати ККС ВС від 29.03.2021 у справі №554/5090/16-к [87]. Правова позиція, викладена у даній постанові, є однією з ключових у зазначеному напрямі. Ототожнення доказу електронної форми, як засобу доказування та матеріального носія такого документа є безпідставним, оскільки характерною ознакою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія. Аналогічного висновку дійшла об'єднана палата ККС ВС у постанові від 25.09.2023 у справі №208/2160/18 [87]. На практиці найпоширенішим доказом електронної форми, який оцінюється на предмет допустимості (або недопустимості), з урахуванням відповідних особливостей, є відеозапис. Відповідно, ВС сформував ширшу практику з цього питання. Зокрема, у постанові від 31.03.2021 р. у справі №333/1539/16-к [87] ВС зазначив, що добровільне надання свідком стороні обвинувачення диска з відеозаписом дорожньо-транспортної пригоди, що було підтверджено ним у судовому провадженні, а не отримання його на підставі тимчасового доступу до речей і документів, не є підставою для визнання такого доказу недопустимим. У іншій ситуації ВС при оцінці релевантної ситуації не погодився з висновками судів першої та апеляційної інстанції щодо визнання недопустимим доказом відеозапису ДТП, отриманого від свідка (постанова від 30.08.2023 у справі №289/445/18 [87]). Зокрема, колегія суддів зазначила, що ототожнення доказу електронної форми, як засобу доказування та матеріального носія такого документа є безпідставним, оскільки характерною ознакою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія. Аналогічна правова позиція, згідно з якою оскільки DVD-R диск з відеозаписом обставин події з камер відеоспостереження був добровільно наданий особою, а тому не було необхідності звертатися з відповідним клопотанням до слідчого судді для отримання копії запису, що не суперечить вимогам КПК України, викладена у постановях ККС ВС від 10.09.2020 у справі №751/6069/19 [87] та від 21.04.2021 у справі № 644/3803/16-к [87]. Схожа позиція щодо оцінки як доказу відеозапису, який є у вільному доступі, викладено у постанові ККС ВС від 30.04.2020 у справі №640/19897/16-к [87]. Для

надання оцінки допустимості як доказу відеозапису, безперечно, необхідно враховувати дотримання порядку його отримання. Класичним прикладом визнання відеозапису недопустимим доказом є його отримання оперативним працівником до внесення відомостей до ЄРДР. Так, ККС ВС у постанові від 07.08.2019 у справі №607/14707/17 [87] зазначив, що отримання оперативним працівником від потерпілого відеодиску суперечить вимогам ч. 1 та ч. 2 ст. 41 КПК України, оскільки оперативний працівник у порушення вимог КПК без доручення слідчого не уповноважений здійснювати процесуальні дії з власної ініціативи, тобто у непередбаченому кримінальним процесуальним законодавством порядку. Водночас необхідно оцінювати обставини отримання оперативним працівником відеозапису у сукупності. Зокрема, надаючи оцінку доводам касаційної скарги захисника щодо недопустимості як доказу протоколу огляду предмета та перегляду відеозапису, з підстав порушення порядку отримання цього доказу (зокрема, жорсткого диска, що оглядався, та відеозапису на ньому), ВС у постанові від 08.02.2023 у справі №201/2609/20 [87] дійшов висновку, що правоохоронні органи безпосередньо мають доступ до системи відеоспостереження «Безпечне місто» і можуть самостійно отримувати з неї інформацію. Тому отримання таких даних оперативним працівником з подальшою їх передачею слідчому не може в цьому випадку розглядатися як порушення норм КПК України встановленого порядку отримання доказу. За аналогічних обставин запис розмов на диктофон (телефон) може бути визнаний як недопустимим, так і допустимим доказом. Зокрема, запис свідком на диктофон розмови з іншою особою визнано як здійснення оперативно-розшукової діяльності за власною ініціативою, що прямо заборонено законом. Враховуючи, що ініціативні дії свідка та потерпілого щодо фіксування розмов на диктофон здійснено без попереднього дозволу суду, ВС дійшов висновку, що цими діями порушені права обвинуваченого, та правильно визнано недопустимими доказами фактичні дані, отримані під час здійснення аудіозаписів розмов свідка з обвинуваченим (постанови ККС ВС від 16.12.2020 у справі №661/4683/13-к [87] та від 15.06.2021 у справі №305/2022/14-к [87]). Водночас є інша позиція щодо оцінки запису телефонної розмови, зробленої на диктофон мобільного телефону

обвинуваченого, який він добровільно видав після його затримання (постанова ККС ВС від 28.01.2021 у справі №182/523/16-к [87]. Цікаву позицію викладено в постанові ККС ВС від 14.04.2021 в справі №288/1418/17 [87]. Судом констатовано, що доводи захисника про недопустимість протоколу проведення слідчого експерименту як доказу винуватості засудженої через відсутність оригінального технічного носія відеозапису, не засновані на приписах закону та не спростовують висновків суду про допустимість цього доказу. Також варто звернути увагу на постанову ККС ВС від 09.04.2020 у справі №727/6578/17 [87] в контексті огляду інформації в телефоні. Перелік доказів електронної форми наведено у постанові ККС ВС від 06.02.2024 у справі №645/6247/16-к [87]. Вартою уваги є ще одна позиція ВС, що сформована в цьому рішенні, що відеозапис слідчої дії є самостійним джерелом доказів. У постанові від 06.02.2024 р. у справі №645/6247/16-к [87] ВС констатував, що технічний носій інформації, на якому зафіксовано проведення слідчого експерименту, а саме його відеозапис, містить достатні відомості, що відображають хід його проведення, що за своєю природою є самостійним джерелом доказів, визначеним ст. 84 КПК України. Також варто звернути увагу на постанову ККС ВС від 27.04.2023 у справі №149/2360/17 [87], відповідно до якої ототожнення доказу електронної форми, як засобу доказування та матеріального носія такого документа є безпідставним, оскільки характерною рисою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія [127, с. 1002-1007]. Хоча певні проблемні питання відображені в окремих рішеннях ВС, нами проведено аналіз практики ВС щодо використання доказів електронної форми в кримінальному процесі України [127, с. 1002-1007], що свідчить про неоднорідність судової практики в досліджуваному питанні.

Під практикою ЄСПЛ як джерелом кримінального процесуального права України пропонується розуміти сукупність рішень ЄСПЛ та Європейської комісії з прав людини постановного характеру, ухвалених по суті справи, що набрали чинності та містять правові позиції, що тлумачать чи уточнюють норми Конвенції та стосуються прав і свобод людини та громадянина [113, с. 17].

Правові акти ЄСПЛ в кримінальному процесі України представлено у вигляді практики ЄСПЛ як джерела кримінального процесуального права України, а також у вигляді рішень ЄСПЛ, у яких встановлено порушення Україною міжнародних зобов'язань (норм КЗПЛ) при вирішенні справ судом, що набрали чинність, як складової кримінального провадження. За результатами даного дослідження встановлено роль практики ЄСПЛ в кримінальному процесі України, що полягає у забезпеченні верховенства права та законності в кримінальному провадженні. Також з'ясовано роль рішення ЄСПЛ, у якому встановлено порушення Україною міжнародних зобов'язань (норм КЗПЛ) при вирішенні справ судом, що набрало чинність, що полягає в ініціюванні механізму забезпечення належного та ефективного захисту прав і свобод людини в кримінальному провадженні [117, с. 239].

Динаміка розвитку кримінального процесуального законодавства України та правова реальність свідчить про посилення ролі та значення практики ЄСПЛ в кримінальному процесі України. Отримані під час дослідження дані обумовлюють: вжиття організаційних та навчальних заходів у напрямку застосування практики ЄСПЛ під час кримінального провадження; проведення подальших, зокрема внутрішньовідомчих, досліджень та моніторингів; вжиття додаткових заходів щодо забезпечення офіційного перекладу рішень ЄСПЛ українською мовою. За результатами дослідження пропонується розробка нових та вдосконалення існуючих електронних інструментів пошуку практики ЄСПЛ та вивчення ефективності її застосування, актуальних як для науковців, так і для практиків, що сприятиме забезпеченню верховенства права та законності під час кримінального провадження [121, с. 14].

Окрему увагу слід звернути на функціональність Базы правових позицій ВС [15], яка виступає інструментом забезпечення однаковості застосування права у сфері доказів електронної форми. Цей ресурс акумулює усталені висновки ВС, що пройшли перевірку на сталість та системність і мають імперативне значення для судів нижчих інстанцій. У контексті роботи судді з доказами електронної форми використання цієї Базы дає змогу: оперативно ідентифікувати правові позиції щодо

допустимості, автентичності та оцінки таких доказів; порівнювати судову практику з метою виявлення відхилень і процесуальних ризиків; формувати обґрунтовані процесуальні рішення з посиланням на єдину практику, що особливо важливо в умовах технологічної складності доказів електронної форми. Практичне застосування Базі особливо цінне для суддів, а також для сторін кримінального провадження в контексті належного обґрунтування рішень щодо доказів електронної форми. При цьому База правових позицій [15] виступає не лише інформаційним, а й методологічним інструментом у роботі суддів.

Отже, роль суду як гаранта процесуальної справедливості є провідною у забезпеченні законності використання доказів електронної форми. Безсумнівно, специфіка цифрових джерел інформації потребує системного переосмислення як в контексті контролю з боку слідчого судді, так і оцінки доказів судом під час судового розгляду. Практика правозастосування вимагає від суду здатності критично аналізувати технічні аспекти доказів електронної форми встановлювати їх автентичність, а також застосовувати норми статей 87, 332, 333, 356 та 360 КПК України, в тому числі — шляхом залучення спеціалістів у сфері ІТ. Визначальним у цій сфері стає рівень цифрової компетентності судді. Проаналізовані освітні програми Національної школи суддів України та наявні методичні матеріали свідчать про поступове розширення знань і навичок суддів щодо роботи з доказами електронної форми. Водночас зберігається об'єктивна потреба у формалізації цих знань через системну спеціалізовану підготовку, уніфікацію підходів до оцінки цифрових об'єктів та впровадження інституційної підтримки (консультацій ІТ-фахівців, створення технічно адаптованих залів засідань тощо).

3.5. Інші учасники кримінального провадження як суб'єкти роботи з доказами електронної форми в кримінальному провадженні

В умовах стрімкого зростання кількості доказів електронної форми у кримінальних провадженнях постає потреба технічного супроводу процесуальної діяльності суб'єктів кримінального процесу. Слідчому, прокурору, адвокату чи судді базових технічних знань уже недостатньо для повноцінної роботи з такими доказами, позаяк вони потребують застосування специфічних складних технічних знань. Це, своєю чергою, зумовлює необхідність залучення до кримінального процесу інших учасників, які володіють відповідними компетентностями, здатні забезпечити належний рівень роботи з доказами електронної форми. У цьому контексті, дослідження ролі технічних фахівців¹⁰ як учасників кримінального провадження набуває особливого значення. Саме ці особи, маючи спеціалізовану освіту та підготовку, здатні дати компетентні відповіді на складні технічні питання, пов'язані з виявленням, фіксацією, зберіганням, перевіркою цілісності та інтерпретацією цифрових слідів.

В. В. Коваленко (2004) зазначає, що спеціальні знання в судочинстві – це наукові та практичні знання й навички, які відповідають сучасному рівню розвитку відповідних галузей людської діяльності (за винятком знань у галузі процесуального та матеріального права), використовуються (застосовуються) при розслідуванні злочинів і судовому розгляді кримінальних справ з метою сприяння слідчому чи суду в збиранні та дослідженні доказів [137, с. 7]. В. Д. Юрчишин (2007) пропонує визначити спеціальні знання як сукупність науково обґрунтованих знань у галузі науки, техніки, мистецтва та ремесла певної особи (спеціаліста) в межах будь-якої професії, які відповідно до норм кримінально-процесуального законодавства є необхідними для повного, всестороннього, об'єктивного встановлення обставин, що входять в предмет доказування та вирішення інших

¹⁰ Термін «технічні фахівці» вжито для позначення осіб, які мають спеціальні знання у сфері інформаційно-комунікаційних технологій, цифрової криміналістики, кібербезпеки, OSINT-аналізу та інших суміжних напрямів, і які залучаються до участі в кримінальному провадженні з метою сприяння у виявленні, фіксації, дослідженні або оцінці доказів електронної форми.

завдань кримінального процесу [298, с. 44]. Науковці звертають увагу на необхідність розрізнявати суб'єктів використання і суб'єктів застосування спеціальних знань, бо «використовувати» і «застосовувати» мають різне значення [137, с. 7–8]. В. І. Чекотило (2015) процесуальними формами використання спеціальних знань у кримінальному процесі називає таке: 1) залучення експерта (статті 69, 242–244, 332 КПК України); 2) залучення спеціаліста (ст. 71 КПК України); 3) витребування висновків ревізій та актів перевірок (ч. 2, 3 ст. 93 КПК України); 4) допит обізнаних осіб (обізнаних свідків та експертів) (ч. 6, 7 ст. 95, ст. 356 КПК України). Інші форми використання спеціальних знань у кримінальному провадженні є непроцесуальними [285, с. 15].

Експерт є одним з ключових технічних фахівців у роботі з доказами електронної форми під час кримінального провадження. Судовий експерт – це не зацікавлена у результатах провадження особа, яка на професійній основі володіє необхідними для вирішення судово-експертних завдань спеціальними знаннями, уміннями та практичними навичками, призначена експертом у порядку, встановленому законом, що прийняла об'єкти експертизи задля проведення дослідження та надання висновку з питань, які виникають під час процесуального провадження і стосуються сфери її знань [85, с. 196].

У сфері роботи з доказами електронної форми експерт є спеціалізованим учасником кримінального провадження, чия діяльність здійснюється відповідно до положень статей 69–70, 242–245 КПК України та Закону України «Про судову експертизу». Відповідно до ч. 1 ст. 69 КПК України експертом у кримінальному провадженні є особа, яка володіє науковими, технічними або іншими спеціальними знаннями, має право відповідно до Закону України «Про судову експертизу» на проведення експертизи і якій доручено провести дослідження об'єктів, явищ і процесів, що містять відомості про обставини вчинення кримінального правопорушення, та дати висновок з питань, які виникають під час кримінального провадження і стосуються сфери її знань [155, с. 1].

Компетенція експерта – це об'єктивна категорія, що має три рівні: процесуальний, науковий, індивідуальний, які охоплюють відповідне коло

експертів: всіх експертів після залучення у кримінальне провадження, експертів певної експертної спеціальності, конкретного експерта. Компетентність експерта поділена на базову, особисту та в конкретній експертизі, котрі характеризують суб'єктивну здатність експерта здійснювати дослідження [296, с. 29].

Механізм залучення експерта до роботи з доказами, зокрема тими, що мають електронну форму, є суворо формалізованим. Так, згідно з ч. 1 ст. 243 КПК України експерт залучається у разі наявності підстав для проведення експертизи за дорученням сторони кримінального провадження. Сторона захисту має право самостійно залучати експертів на договірних умовах для проведення експертизи, у тому числі обов'язкової. Також експерт може бути залучений слідчим суддею за клопотанням сторони захисту у випадках та порядку, передбачених статтею 244 КПК України. Отже, під час досудового розслідування підставою для проведення експертизи може бути відповідна постанова слідчого чи прокурора, ухвала слідчого судді або ж відповідне доручення сторони захисту.

Водночас ст. 332 КПК України передбачає можливість проведення експертизи за ухвалою суду – під час судового розгляду суд за клопотанням сторін кримінального провадження або потерпілого за наявності підстав, передбачених ст. 242 КПК України, має право своєю ухвалою доручити проведення експертизи експертній установі, експерту або експертам. Також суд має право своєю ухвалою доручити проведення експертизи експертній установі, експерту або експертам незалежно від наявності клопотання сторін, згідно з ч. 2 ст. 332 КПК України.

Відповідно до ч. 2 ст. 9 Закону України «Про судову експертизу», особа або орган, які призначають або замовляють судову експертизу, можуть доручити її проведення тим судовим експертам, яких внесено до державного Реєстру атестованих судових експертів, або іншим фахівцям з відповідних галузей знань, якщо інше не встановлено законом. Тобто, за загальним правилом, проведення експертизи в кримінальному провадженні може бути долучено лише експерту, якого внесено до Реєстру атестованих судових експертів. В іншому ж випадку залучення особи, яку не внесено до реєстру, необхідно буде детально

обґрунтовувати, і це може надалі розглядатися судом в контексті допустимості отриманого таким чином висновку експерта як доказу.

М. Г. Щербаковський (2016) окреслює основні напрями використання судових експертиз у кримінальному провадженні: 1) кримінально-правовий (встановлення ознак, об'єкта, предмета, суб'єкта, об'єктивної та суб'єктивної сторін злочину); 2) кримінально-процесуальний (отримання нових доказів, перевірка наявних доказів, формування сукупності доказів, обґрунтування процесуальних рішень); 3) криміналістичний (висування та перевірка версій, моделювання та реконструкція об'єктів, процесів, явищ, ідентифікація осіб та предметів, подолання протидії розслідуванню, планування); 4) кримінологічний (встановлення обставин, що сприяли вчиненню злочинів) [296, с. 32–33].

У межах кримінального провадження, яке передбачає дослідження доказів електронної форми завданням експерта є проведення експертизи, переважно комп'ютерно-технічної або телекомунікаційної. Враховуючи необхідність наявності формальної підстави для проведення експертизи у формі процесуального документа, в якому мають бути визначені завдання, що підлягають вирішенню експертом, розглянемо детальніше вказані вище види експертиз.

Комп'ютерно-технічна експертиза – експертиза, що належить до виду інженерно-технічних експертиз, об'єктом дослідження якої є комп'ютерна техніка та (або) комп'ютерні носії інформації [6, с. 146-149; 264, с. 318]. Відповідно до підпункту 1.2.2 Інструкції про призначення та проведення судових експертиз видом експертизи є інженерно-технічна, а підвидом – комп'ютерно-технічна, тобто під час призначення експертизи експерту може вказуватись лише інженерно-технічна експертиза (вид) та комп'ютерно-технічна (підвид) [163, с. 37]. Комп'ютерно-технічна експертиза проводиться з метою: визначення статусу об'єкта як комп'ютерного засобу, виявлення і вивчення його ролі в розслідуваному злочині, а також отримання доступу до інформації на електронних носіях з подальшим всебічним її дослідженням. До основних завдань комп'ютерно-технічної експертизи належать: установлення робочого стану комп'ютерно-технічних засобів; установлення обставин, пов'язаних з використанням комп'ютерно-

технічних засобів, інформації та ПЗ; виявлення інформації та ПЗ, що містяться на комп'ютерних носіях; встановлення відповідності програмних продуктів певним версіям чи вимогам на їх розробку [264, с. 318-319]. Питання, що вирішуються при проведенні комп'ютерно-технічної експертизи містять відповідні методичні рекомендації та спеціалізовані видання [91, с. 2–3]. Б. Б. Теплицький (2018) формулює такі основні вимоги до питань, які ставлять для проведення комп'ютерно-технічної експертизи: 1) під час постановки питань необхідно використовувати усталений понятійний апарат, уникаючи жаргонізмів та напівпрофесійних термінів; 2) питання мають бути максимально чіткими й передбачати можливість надання судовим експертом однозначної відповіді; 3) формулювання питання не повинно стосуватися етапів дослідження інформації; 4) питання не мають носити довідковий характер; 5) питання не повинні мати правовий характер і сягати за межі компетенції судового експерта певної експертної спеціальності; 6) питання мають відповідати сучасній методичній і технічній базі, доступній судовому експерту; 7) питання повинні бути спрямовані на встановлення конкретних обставин події, що належать до предмета доказування; 8) питання доцільно ставити так, щоб під час виконання конкретних завдань розслідування витрати на проведення досліджень були мінімальними [266, с. 309].

Проте методичними рекомендаціями Міністерства юстиції України визначено завдання експертизи комп'ютерної техніки та орієнтовний перелік питань. До завдань віднесено встановлення робочого стану комп'ютерно-технічних засобів; встановлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та ПЗ; виявлення інформації та ПЗ, що містяться на комп'ютерних носіях; встановлення відповідності програмних продуктів певним версіям чи вимогам на його розроблення. Звісно, орієнтовний перелік питань у методичних рекомендаціях сформульовано у досить загальних термінах, а формулювання питань є відкритим [163, с. 38].

Телекомунікаційна експертиза – це вид інженерно-технічних експертиз, змістом якої є дослідження експертом на основі спеціальних знань у галузі електроніки і телекомунікаційних систем, засобів, мереж та їх складових частин,

інформації, що ними передається, приймається, обробляється та містить фактичні дані про обставини, що мають значення для органів досудового розслідування та суду [264, с. 320]. В. А. Коршенко (2017) розглядає судову телекомунікаційну експертизу вид інженерно-технічних експертиз, змістом якої є дослідження експертом на основі спеціальних знань у галузі електроніки і телекомунікацій систем, засобів, мереж та їх складових частин, інформації, що ними передається, приймається, обробляється та містить фактичні дані про обставини злочину, що мають значення для кримінального провадження [149, с. 15–16]. Завданнями телекомунікаційної експертизи є таке: визначення характеристик та параметрів телекомунікаційних систем та засобів; установлення фактів та способів передачі (отримання) інформації в телекомунікаційних системах, фактів та способів доступу до систем, ресурсів та інформації у сфері телекомунікацій; визначення технічних показників якості надання телекомунікаційних послуг на рівні їх споживання; встановлення конфігурації та робочого стану телекомунікаційних систем та засобів; типу, марки, моделі та інших класифікаційних категорій телекомунікаційних систем та засобів; дослідження алгоритмів обробки інформації та її захисту у сфері телекомунікацій [264, с. 322]. Питання, що вирішуються при проведенні телекомунікаційної експертизи містять відповідні методичні рекомендації та спеціалізовані видання [6, с. 149-151; 264, с. 323].

Ефективним способом організації розслідування злочинів, вчинених із використанням телекомунікаційних технологій, є технічне супроводження кримінального провадження одними і тими самими фахівцями, а також понятими, які мають елементарні знання щодо функціонування телекомунікаційних засобів. Під час проведення огляду місця події та обшуку слід обов'язково залучати спеціалістів у галузі телекомунікаційних систем, електронно-обчислювальної техніки, радіотехніки, програмування тощо. Якщо працюючий телекомунікаційний засіб неможливо вичленувати з мережі, то телекомунікаційна експертиза призначається на місці проведення слідчої дії [149, с. 17].

Найбільш формалізованим способом документування участі технічних фахівців у кримінальному провадженні є висновок експерта. Згідно з ч. 2 ст. 84

КПК України висновок експерта це один із процесуальних самостійних джерел доказів, нарівні з показаннями, речовими доказами та документами.

Методологічні та правові стандарти роботи експерта є чітко визначеними. Відповідно до ч. 5 ст. 8 Закону України «Про судову експертизу» методики проведення судових експертиз (крім судово-медичних та судово-психіатричних) підлягають атестації та державній реєстрації в порядку, встановленому Кабінетом Міністрів України [235, с. 1], а саме відповідно до Порядку атестації та державної реєстрації методик проведення судових експертиз, затверджений постановою Кабінету Міністрів України від 02.07.2008 р. № 595 [217, с. 1].

Порядок ведення Реєстру методик проведення судових експертиз, затверджений наказом Міністерства юстиції України від 02.10.2008 № 1666/5 [218], становить нормативно-правову основу для ведення централізованого обліку методик, що застосовуються у судово-експертній діяльності. Цей нормативний акт забезпечує контроль за легітимністю, актуальністю та науковою обґрунтованістю методик, сприяє уніфікації експертної практики. Реєстр методик є системним елементом нормативного регулювання, який доповнює Інструкцію про призначення та проведення судових експертиз та експертних досліджень, затверджену Наказом Міністерства юстиції України від 08.10.1998 № 53/5 [90, с. 1]. Застосування зазначених стандартів забезпечує наукову обґрунтованість, відтворюваність, об'єктивність та належну фіксацію процедур. Це є необхідною умовою визнання висновку експерта допустимим доказом, що може бути використаний у кримінальному провадженні.

Важливо зауважити, що всі експертні дослідження та дії з цифровими даними здійснюються виключно з використанням криміналістичних копій (криміналістичних образів), наданих для дослідження електронних носіїв інформації, а не з оригінальними пристроями чи носіями. Робота з оригіналом електронного носія інформації не здійснюється (що передбачено відповідною методологією) через те, що здатне вплинути на цілісність даних.

Допит експерта в суді є важливим етапом. Відповідно до ч. 1 ст. 356 КПК України за клопотанням сторони кримінального провадження, потерпілого або за

власною ініціативою суд має право викликати експерта на допит для роз'яснення висновку.

Мета допиту експерта полягає у роз'ясненні, уточненні та доповненні складеного ним висновку для усунення його незрозумілості або неповноти. Роз'яснення висновку експерта являє собою пояснення його змісту у цілому або окремих частин, спрямоване на формування в учасників кримінального провадження правильного їх розуміння. Уточнення висновку експерта передбачає здійснення додаткової аргументації окремих його положень з метою надання їм більш детальної конкретизації. Доповнення висновку експерта передбачає поглиблення змісту окремих його частин шляхом формулювання та обґрунтування експертом додаткових тверджень, які не носять характеру висновків, ґрунтуються на результатах проведеного дослідження та не потребують додаткових досліджень [36, с. 181]. М. Г. Щербаковський (2016) вказує, що предмет допиту експерта охоплює предмет експертизи та додаткову інформацію, яка впливає із проведеного дослідження [296, с. 32]. Тоді як А. Р. Воробчак (2019) переконаний, що предметом допиту експерта охоплюються такі групи даних: 1) щодо методики дослідження і теоретичних розробок, використаних під час проведення експертизи; 2) про достатність відомостей, на підставі яких готувався висновок; 3) щодо наукового обґрунтування та методів, за допомогою яких експерт дійшов висновку, а також застосованих ним засобів; 4) про застосовність і правильність застосування принципів та методів до фактів кримінального провадження; 5) відомості, необхідні для з'ясування причин неповноти або суперечливості висновку експерта [36, с. 181–182].

Безперечно, залежно від конкретної ситуації розслідування може виникати потреба в значній кількості експертних досліджень за різними експертними спеціальностями (видами та підвидами судових експертиз), які мають свої особливості, до того ж проводяться інколи різними експертними установами чи підрозділами та впродовж тривалого часу [267, с. 213].

Проблемним аспектом сучасної практики є тривалі строки проведення комп'ютерно-технічних експертиз. Така ситуація зумовлюється, зокрема, значним

обсягом завдань, що покладаються на експертів у сфері дослідження електронних носіїв інформації, обмеженою кількістю експертів відповідної спеціалізації, а також складністю технічних процедур, пов'язаних із вилученням, копіюванням та аналізом інформації. Затягування строків виконання експертизи може негативно впливати на ефективність досудового розслідування, створювати ризики втрати або зміни цифрових слідів та обмежувати можливості сторін щодо своєчасного подання або спростування доказів. У цьому контексті актуальним є питання оптимізації процесу призначення та виконання комп'ютерно-технічних експертиз, зокрема шляхом чіткого розмежування компетенції експертів і спеціалістів, а також удосконалення матеріально-технічної бази експертних установ.

Важливим напрямом удосконалення механізму залучення технічних фахівців у кримінальному провадженні є чітке розмежування повноважень та функцій, що належать до компетенції спеціаліста, і тих, що віднесені до компетенції експерта. Такий підхід сприятиме оптимізації розподілу процесуального навантаження, дозволить уникнути дублювання завдань та забезпечить більш ефективне використання кадрового потенціалу експертних установ. Практика діяльності криміналістичної ІТ-лабораторії НАБУ [46; 47] свідчить, що залучення спеціалістів для виконання первинних технічних дій — таких як фіксація цифрових слідів, створення криміналістичних копій носіїв інформації, попередній аналіз метаданих — дозволяє значно скоротити обсяг робіт, безпосередньо виконуваних експертами, та зосередити їх на проведенні глибоких досліджень і формулюванні висновків, що мають процесуальне значення у розумінні ст. 84 КПК України. Такий розподіл функцій відповідає як вимогам процесуальної економії, так і стандартам належної організації судово-експертної діяльності.

На нашу думку, перевантаженість експертів, які проводять комп'ютерно-технічні експертизи, має місце сьогодні через те, дуже часто експерту ставлять завдання, які цілком можуть бути реалізовані за участі спеціаліста. Яскравим прикладом є призначення експертизи для пошуку певних відомостей серед масиву цифрових даних, збережених в комп'ютерній системі або на ЕНІ, вилучених під час обшуку. Але ж під час проведення огляду слідчий або прокурор разом зі

спеціалістом можуть виготовити криміналістичну (побітову) копію інформації з оригінального носія та дослідити цю копію, відшуковуючи інформацію, що цікавить слідчого. Ба більше, такий алгоритм роботи передбачає, що слідчий може одразу коригувати напрямок пошуку інформації, що здійснює спеціаліст, формуючи додаткові запити з урахуванням вже відшуканих даних, уточнювати ці запити або ж кардинально змінювати їх на основі оперативної інформації, що надійшла ледь не щойно. Такий огляд оформляється шляхом складання протоколу огляду документа (комп'ютерних даних), в якому фіксуються всі дії слідчого або прокурора та спеціаліста, і він є доказом у кримінальному провадженні. Перевагою пропонованого є швидкість проведення (порівняно з експертизою), гнучкість та результативність, можливість оперативно приймати рішення з урахуванням щойно здобутої інформації, а також необмежена кількість повторів відповідного огляду з урахуванням нових доказів у кримінальному провадженні. Якщо ж з певних причин принциповим є отримання саме висновку експерта (окремі суди та судді орієнтують сторону обвинувачення на необхідність здобуття такої категорії доказів саме за результатами проведення експертизи) для встановлення факту наявності відповідної інформації, то за результатами проведення описаного вище огляду слідчим, прокурором може бути призначено проведення відповідної експертизи. Та вже ж питання в цій експертизі буде сформульовано з урахуванням встановлених відомостей, що значно підвищить результативність експертного дослідження, а експерт отримає не просто електронний носій інформації, що припав пилі, адже не чіпався з моменту обшуку, а той же носій інформації разом з протоколом огляду його криміналістичної копії, що значно спростить підготовку висновку експерта. Бо в цьому разі експерт не «копирсатиметься» в цифрових даних сам, а фактично перевірятиме «роботу» слідчого або прокурора, виконану зі спеціалістом, і тоді вже або підтвердить встановлені дані, або спростує. Але це більше про стратегію представлення суду «найкращого» доказу та слідування усталеним практикам, а не про ефективне використання ресурсів держави під час досудового розслідування. У разі ж проведення такого пошуку лише шляхом призначення експертизи експерт так само виготовить криміналістичну копію інформації з оригінального носія та

дослідить цю копію, відшуковуючи інформацію виключно відповідно до питань, визначених слідчим чи прокурором питань у постанові про призначення експертизи. Після чого експерт сформує висновок і скерує його слідчому чи прокурору. Відповідні дії, з урахуванням завантаженості експерта, потенційно можуть тривати місяці, а то й роки. Як наслідок, буде витрачено цінний ресурс експерта на досить просту дію і при цьому буде досягнуто значно менш ефективного результату (адже пошук здійснюватиметься виключно за поставленими питаннями) і в значно довші строки. У разі встановлення слідчим у висновку експерта даних, що потребують проведення додаткового пошуку), що досить вірогідно, й призначення нової експертизи, процес триватиме ще довше.

Зважаючи на це, перший шлях вбачається значно ефективнішим. Стратегія з проведенням умовно простих комп'ютерно-технічних досліджень працювала на початку 2000-х років, коли таких запитів були сотні, але вона не працює тепер, коли їх тисячі.

Відповідно до ч. 1 ст. 71 КПК України спеціалістом у кримінальному провадженні є особа, яка володіє спеціальними знаннями та навичками й може надавати консультації, пояснення, довідки, висновки та інші документи під час досудового розслідування і судового розгляду з питань, що потребують відповідних спеціальних знань і навичок.

У разі необхідності та за наявності підстав може бути залучено з іноземної держави, міжнародної організації як спеціаліста фахівця у галузі хімічної, біологічної, радіаційної, ядерної чи іншої зброї (абз. 2 ч. 1 ст. 71 КПК України).

В. О. Яремчук (2014) пропонує класифікувати функції спеціаліста залежно від: а) вербальності чи невербальності слідчої (розшукової) дії; б) часу здійснення ним функцій; в) характеру, виду і роду його діяльності; г) завдань, на вирішення яких спрямовані дії спеціаліста. Дослідниця узагальнює форми допомоги спеціаліста під час слідчої (розшукової) дії: 1) організаційно-технічна, яка охоплює підготовчу, технічну, організаційну; 2) пошукова; 3) інформаційна; 4) консультативна; 5) аналітична і 6) надання «висновку спеціаліста» [299, с. 15].

Права та обов'язки спеціаліста визначено ч. 4 та ч. 5 ст. 71 КПК України відповідно. У контексті роботи з доказами електронної форми роль спеціаліста є критично важливою на первинних стадіях збору та фіксації цифрових слідів, де порушення процедури навіть на технічному рівні може призвести до втрати доказу. Залучення спеціаліста на цих етапах дозволяє забезпечити відповідність процедур збирання доказів вимогам цілісності, незмінності та достовірності, що є критеріями допустимості згідно з ч. 1 ст. 87 КПК України.

Механізм залучення спеціаліста досить чітко визначений законодавцем. Відповідно до ч. 2 ст. 71 КПК України спеціаліст може бути залучений для надання безпосередньої технічної допомоги (фотографування, складення схем, планів, креслень, відбір зразків для проведення експертизи тощо) сторонами кримінального провадження під час досудового розслідування і судом під час судового розгляду, а також для надання довідок, висновків та інших документів у випадках, передбачених п. 7, п. 8, п. 9 ч. 4 ст. 71 КПК України.

Механізм залучення спеціаліста до кримінального провадження у справах, де фігурують докази електронної форми має подвійний характер: з одного боку, він ґрунтується на процесуальній ініціативі сторони чи суду; з іншого — на володінні особою спеціальними знаннями та відповідності формальним вимогам.

З огляду на технічну специфіку об'єктів цифрового середовища, що підлягають дослідженню, особливого значення набуває питання про належну перевірку фаховості та об'єктивності спеціаліста, якого планується залучити до кримінального провадження. Йдеться, зокрема, про обов'язкову перевірку: а) наявності професійної сертифікації в галузі цифрової криміналістики або суміжних сфер; б) документально підтвердженого досвіду в проведенні досліджень електронних носіїв інформації; в) належності до компетентної установи (експертна установа, науковий центр, навчальний заклад, технічна лабораторія) або до суб'єкта ринку (офіційний провайдер, ліцензована компанія тощо).

Методологічні та правові стандарти роботи спеціаліста під час кримінального провадження з доказами електронної форми не визначені в КПК України, іншому законі чи підзаконному акті, однак врегульовані на рівні ДСТУ.

Фундаментальним документом, що регламентує порядок дій спеціалістів при роботі з комп'ютерними системами та електронними носіями інформації, є ДСТУ ISO/IEC 27037:2017. У цьому контексті спеціаліст виконує одну з ключових ролей у межах моделі Digital Evidence First Responders (DEFR) — тобто осіб, які першими взаємодіють з цифровими джерелами інформації під час кримінального провадження. Перший контакт з цифровим об'єктом має саме залучений слідчим, прокурором спеціаліст, на нього покладено обов'язок з ідентифікації, ізоляції, фіксації та безпечного вилучення комп'ютерної системи або копіювання інформації, що в майбутньому може стати доказом. Тут важливо зазначити, що DEFR має забезпечити досить специфічні технічні вимоги ДСТУ ISO/IEC 27037:2017, а такою особою може бути як слідчий, так і прокурор, як оперативний працівник, так і залучений стороною обвинувачення спеціаліст. Очевидно, що слідчому або прокурору реалізувати вказані технічні вимоги проблематично через відсутність (переважно) необхідної технічної кваліфікації, тобто залучення спеціаліста в сфері цифрової криміналістики необхідне стороні обвинувачення для дотримання технічних вимог під час пошуку та фіксації доказів електронної форми.

У випадках, коли до провадження залучається спеціаліст, його участь фіксується шляхом відображенні в протоколі слідчої (розшукової) чи процесуальної дії, допускається долучення письмових пояснень спеціаліста чи технічної довідки, так само участь спеціаліста під час судового провадження фіксується в журналі судового засідання.

Документування дій спеціаліста в кримінальному процесі здійснюється у формі: висновку спеціаліста (ч. 3 ст. 214, ч. 3 ст. 245-1, п. 9 ч. 4 ст. 71 КПК України); протоколу слідчої (розшукової) дії (наприклад, огляду, обшуку, тимчасового доступу до речей і документів); в журналі судового засідання — у разі його залучення в судовому розгляді; додаткових технічних документах, таких як: довідки щодо конфігурації пристрою, лог-файли, звіти системної активності, витяги з реєстрів або журналів подій. Вони можуть долучатися до матеріалів кримінального провадження як додатки до протоколу відповідно до вимог ст. 104 КПК України.

Б. Б. Теплицький (2021) зазначає, що особливістю розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є обов'язкове залучення як спеціаліста фахівця (фахівців) у галузі використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Залежно від конкретної ситуації, це може бути як судовий експерт за напрямом комп'ютерно-технічної та (або) телекомунікаційної експертизи, так й інші особи, які володіють відповідними спеціальними знаннями та навичками використання техніко-криміналістичних засобів, наприклад, фахівець з експлуатації або створення конкретних програмних засобів або ж з технічної експлуатації і ремонту певного обладнання [267, с. 211-212].

Під час судового розгляду сторони кримінального провадження мають право заявляти клопотання про залучення спеціаліста або використання його пояснень і допомоги (ч. 3 ст. 71 КПК України). Так, спеціаліст може бути залучений судом під час судового розгляду для безпосереднього надання технічних консультацій чи застосування програмних або технічних засобів під час судового розгляду, що не пов'язано з його діяльністю під час досудового розслідування. Предметом такого пояснення може бути, наприклад: роз'яснення характеристик та особливостей різних форматів цифрових даних (наприклад, особливості метаданих PDF-документів, розширень файлів, форматів логів); характеристика типів цифрових носіїв (твердотілі накопичувачі, зовнішні жорсткі диски, флешпам'ять, RAID-масиви тощо); пояснення алгоритмів шифрування або збереження даних (AES, RSA, алгоритми ключового обміну тощо); опис специфіки мережевої взаємодії, наприклад, шляхи передачі електронної пошти, обміну файлами через хмарні сервіси, використання VPN-тунелів тощо.

Залучення спеціаліста на стадії судового розгляду дозволяє суду правильно інтерпретувати технічні параметри цифрових об'єктів, які інакше можуть бути недоступні для повноцінної оцінки у межах юридичної компетенції. Це сприяє реалізації принципу об'єктивної істини та забезпеченню належного рівня правового аналізу.

У КПК України немає прямої норми, яка б передбачала можливість допиту спеціаліста в суді щодо технічних обставин отримання або аналізу доказів, як це визначено ч. 1 ст. 356 КПК України щодо допиту експерта для роз'яснення його висновку. Оскільки аналогічної норми щодо спеціаліста немає, законне залучення спеціаліста до надання пояснень у суді можливе лише у двох формах: 1) виклик спеціаліста як свідка, але в такому разі його показання не будуть мати особливого процесуального статусу, як у експерта; 2) повторне залучення спеціаліста для використання його пояснень і допомоги під час судового розгляду (наприклад, повторний огляд, демонстрація доказів електронної форми тощо).

На жаль, досі в органах досудового розслідування бракує достатньої кількості фахівців, які можуть бути залучені як спеціалісти – особа, яка є експертом, котрий проводить комп'ютерно-технічні експертизи, теоретично може бути залучена як спеціаліст. Невирішеним залишається питання оплати роботи спеціалістів з приватного сектору, яких залучає сторона обвинувачення.

Дослідивши питання можливості фіксації в протоколі слідчої дії консультацій і пояснень, які дають спеціалісти з приводу спеціальних питань при проведенні слідчих дій, В. В. Коваленко підтримує пропозицію С. Д. Коберника та інших науковців про запровадження спеціального додатку до протоколів слідчих дій, проведених за участю спеціалістів. Такий додаток запропоновано іменувати Технологічною картою спеціаліста (криміналіста, автотехніка, судового медика тощо). Заповнювати технологічну карту повинен сам спеціаліст із зазначенням умов і результатів застосування НТЗ [137, с. 8]. В. О. Яремчук (2014) висловлює критичні міркування щодо норми, яка передбачає можливість спеціалісту керуватися у своїх діях вказівками сторони захисту, що його залучила [299, с. 15]. Однак це право сторони захисту очевидно має бути адекватно забезпечено.

Отже, спеціаліст — це процесуальна фігура із важливими технічними функціями, яка не може підміняти експерта у процесі доказування, проте забезпечує передумови для належного збирання, збереження та тлумачення доказів електронної форми.

У зв'язку з розширенням інформаційних можливостей суспільства та доступністю цифрових технологій у кримінальному процесі України зростає роль даних, отриманих із відкритих джерел (open source intelligence, OSINT). Особливої уваги заслуговує діяльність спеціалізованих неурядових організацій, зокрема, міжнародної спільноти Bellingcat, української ініціативи InformNapalm, а також аналітичної структури Digital Forensic Research Lab (DFRLab). Зазначені організації здійснюють незалежні розслідування, ґрунтуючись виключно на відкритих цифрових джерелах, з дотриманням публічної верифікації, документування та аналізу цифрових слідів. У межах кримінального провадження в Україні представники таких організацій можуть набувати статусу спеціаліста або свідка, залежно від обставин справи.

OSINT-аналітик може залучатися до участі в проведенні слідчих (розшукових) дій, наприклад огляду, як спеціаліст. Участь таких фахівців у ролі спеціаліста обвинувачення часто трапляється у справах, що мають міжнародний резонанс або стосуються воєнних злочинів, кіберзлочинності та гібридних загроз, що особливо актуалізувалося з початком повномасштабного російського вторгнення. Результати OSINT-аналізу часто оформлюються як огляд (протоколом огляду) та можуть бути доказами відповідно до ст. 84 КПК України.

За результатами залучення представників громадських організацій або незалежних аналітичних структур як спеціалістів, поряд з загальними вимогами до фіксації результатів роботи спеціалістів у кримінальному провадженні, важливим є аналітичний звіт, що містить: опис методики верифікації (геолокаційна перевірка, крос-джерельний аналіз, обробка метаданих), переліки джерел (URL, ґеші, цифрові сліди), часову шкалу подій, скриншоти екранів і результати аналізу. Протокол Берклі встановлює, що такі звіти повинні містити послідовність логічних кроків та збереження всіх проміжних результатів для підтвердження автентичності отриманої інформації.

Під час роботи з відкритими джерелами, особливо у сфері OSINT, ключовим орієнтиром для технічних учасників виступає Протокол Берклі. Цей протокол не є НПА у національному праві, однак містить чіткі методичні вимоги щодо

достовірності, автентичності, ідентифікованості та відтворюваності інформації з відкритих джерел, що набуває особливої ваги при залученні технічних звітів OSINT-груп (див. підрозділ 4.1). При цьому процесуальна допустимість таких даних значною мірою залежить від якості їх документування, основні положення останнього і визначені в Протоколі Берклі.

Проблемним питанням дотепер залишається сертифікація таких OSINT-аналітиків як спеціалістів та підтвердження їх кваліфікації.

Особливої актуальності з початком повномасштабного російського вторгнення набула діяльність неурядових організацій та окремих осіб, у т. ч. адвокатів, що з 2014 року займаються документуванням порушень міжнародного гуманітарного права та міжнародного права прав людини. Документування порушень міжнародного права, що здійснюється неурядовими організаціями та окремими фізичними особами, полягає у збиранні та збереженні інформації, яка може мати значення для притягнення до відповідальності, зокрема для притягнення до кримінальної відповідальності причетних до цих порушень осіб. Зібрана і збережена документаторами інформація може бути отримана слідчим, прокурором від документаторів або витребувана у них на підставі ч. 2 ст. 93 КПК України і надалі набути значення доказів [185, с. 77–78].

Отже, участь технічних фахівців у кримінальному провадженні зумовлена об'єктивною потребою у використанні суб'єктами кримінального провадження спеціальних знань технічного характеру для забезпечення належної процесуальної роботи з доказами електронної форми. До цієї категорії осіб відносяться експерти, спеціалісти, аналітики та інші фахівці, компетентні в галузях ІТ, телекомунікацій, комп'ютерної безпеки, цифрової криміналістики тощо. Їхня участь на всіх стадіях кримінального провадження забезпечує об'єктивність здобуття, збереження, обробки, аналізу та інтерпретації доказів електронної форми. Технічні фахівці посідають автономне та водночас інтегроване місце в системі кримінального провадження, забезпечуючи його технологічну спроможність і сприяючи досягненню завдань кримінального процесу в умовах цифрової трансформації.

РОЗДІЛ 4. МІЖНАРОДНІ ПРОЦЕДУРИ ПОШУКУ, ФІКСАЦІЇ ТА ВИКОРИСТАННЯ ДОКАЗІВ ЕЛЕКТРОННОЇ ФОРМИ

4.1. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних (Berkeley Protocol on Digital Open Source Investigations) та застосування його вимог під час кримінального провадження

Стрімкий розвиток цифрових технологій та соціальних мереж спричинили появу нових можливостей документування злочинів міжнародного та національного характеру. Значна частина інформації про воєнні злочини та інші правопорушення нині фіксується громадянами, журналістами та правозахисниками, що надає такому матеріалу потенціал доказу у кримінальному процесі. Водночас він потребує перевірки достовірності, встановлення автентичності та належної фіксації.

З огляду на ці виклики у 2020 році Центр прав людини Юридичного факультету Берклі спільно з Управлінням ООН з прав людини розробили Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних [238] (Berkeley Protocol on Digital Open Source Investigations). Він містить міжнародні стандарти для проведення онлайн-досліджень щодо ймовірних порушень міжнародного права у галузі прав людини та міжнародного гуманітарного і кримінального права. Також викладені вказівки щодо методологій та процедур збору, аналізу та збереження цифрової інформації у професійному, юридичному та етичному порядку. Протокол Берклі встановлює заходи, які онлайн-слідчі можуть вжити для захисту цифрової, фізичної та психосоціальної безпеки для себе та інших, включаючи свідків, жертв та осіб, які надають першу допомогу (наприклад, громадян, активістів та журналістів), які ризикують власною безпекою і документують порушення прав людини та серйозні порушення міжнародного права. Протокол Берклі йде слідами двох попередніх протоколів Організації Об'єднаних Націй: Міннесотського протоколу з розслідування потенційно

незаконного позбавлення життя (1991, оновлено у 2016 р.) та Посібника з питань ефективного розслідування і документування фактів катувань та іншого жорстокого, нелюдського чи такого, що принижує гідність, поводження або покарання (Стамбульський протокол) (1999, оновлено у 2004 р.).

Хоча керівні принципи й навчання з використання спеціальних інструментів та ПЗ є суттєвою частиною покращення якості розслідувань з використанням відкритих цифрових даних, Протокол Берклі зосереджується не на конкретних технологіях, платформах, ПЗ чи інструментах, а скоріше на основних принципах та методологіях, які можна послідовно застосовувати навіть при зміні самої технології. Ці принципи визначають мінімальні правові та етичні стандарти для проведення ефективних розслідувань з використанням даних у відкритому доступі. Дотримуючись вказівок Протоколу Берклі, слідчі зможуть забезпечити якість своєї роботи, мінімізуючи при цьому фізичні, психосоціальні та цифрові ризики для себе та інших [273, с. 39].

Протокол Берклі визначає цифрову інформацію, отриману з відкритих джерел (цифрова інформація у відкритому доступі) як інформацію, що є у відкритому доступі в інтернеті, до якої можна отримати доступ, наприклад, на загальнодоступних вебсайтах, в інтернет-базах даних або на платформах соціальних медіа. Але на практиці спостерігається різне розуміння відкритих джерел та їх перелік. У Протоколі Берклі йдеться про відкритий код, відкрите ПЗ як дозволені «інструменти» для пошуку, збирання, збереження цифрової інформації у відкритому доступі. Відкритий код, відкрите ПЗ – побудоване з вихідного коду, який кожен, хто має доступ, може перевірити, змінити чи покращити. Код не бачать користувачі, але він підпадає під вказані маніпуляції програмістом. На відкрите ПЗ не поширюються авторські права, патенти чи інші юридичні засоби контролю [238, с. 25, 27].

А ось деякі дослідники пропонують свій авторський підхід, який ми теж підтримуємо: відкриті джерела цифрової інформації – це медіа, соціальні медіа, вебсайти, геопросторові платформи, бази даних, офіційні дані та інші платформи, на яких можна спостерігати, купувати, або запитувати загальнодоступну

інформацію [18, с. 233]. При цьому І. В. Басиста, Л. В. Гаврилук, А. В. Гутник, А. Я. Хитра (2024) наголошують, що з відкритих джерел все ж отримуємо інформацію, а не докази [18, с. 236], що, на нашу думку, також слушно.

Використання інформації з відкритих джерел у кримінальному провадженні демонструє їх значення насамперед на етапі розслідування, коли необхідно швидко встановити фактичні дані про подію злочину та коло причетних осіб. Проте відсутність у КПК України уніфікованих процедур перевірки та фіксації такої інформації призводить до ситуацій, коли зібрані матеріали ризикують не відповідати критеріям допустимості. У цьому контексті положення Протоколу Берклі виступають необхідним орієнтиром для слідчих і прокурорів, оскільки забезпечують методологічну основу для фіксації, перевірки та збереження цифрової інформації з відкритих джерел, що підвищує якість та результативність розслідування.

Ще у 2021 році ОГП започаткував практику огляду цифрової інформації з відкритих джерел даних (мережі Інтернет) з урахуванням стандартів, викладених у Протоколі Берклі. Зокрема, у червні 2021 року керівникам обласних прокуратур був скерований лист-орієнтування «Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел» і вказано на необхідність вжити відповідних заходів для орієнтування прокурорів і працівників слідчих підрозділів правоохоронних органів на впровадження у практичну діяльність запропонованої методики проведення оглядів цифрової інформації з відкритих джерел даних. Для самостійного опрацювання та використання у роботі до цього листа додано офіційний переклад Протоколу Берклі. Тож, вважаємо, ОГП приділяє належну увагу методологічному забезпеченню прокурорів щодо фіксації цифрової інформації з відкритих джерел.

Фіксація інформації з відкритих джерел під час кримінального провадження здійснюється шляхом проведення огляду в порядку ст. 237 КПК України. Проводячи вказану слідчу дію відповідно до вимог статей 223, 237 КПК України, в обов'язковому порядку необхідно на підставі ст. 71 цього Кодексу залучати спеціаліста, який має вищу освіту у сфері інформаційних систем та технологій, для

визнання надалі судом інформації, що міститься в електронному документі, виготовленому в такий спосіб, як оригіналу відповідно до ч. 4 ст. 99 КПК України. У разі проведення огляду іноземних джерел відкритої інформації слід також, керуючись положеннями ст. 68 КПК України, залучати до проведення цієї слідчої дії перекладача.

Для фіксації інформації з відкритого джерела під час кримінального провадження в протоколі огляду необхідно відобразити всі відомості, визначені в п. 155 Протоколу Берклі. З метою уніфікації правозастосовної практики пропонується розроблений нами зразок протоколу огляду (див. Додаток Ж).

Варто зауважити, що на практиці Протоколами Берклі слідчі та прокурори почали називати протоколи огляду інформації з відкритих джерел, здійснені в порядку ст. 237 КПК України, часто не усвідомлюючи про що саме йде мова й діючи шляхом буквального відтворення запозиченого у колег зразка без усвідомлення суті та специфіки здійснюваної ними слідчої (розшукової) дії. І це ще раз підтверджує необхідність системного самостійного навчання й самовдосконалення та профільного підвищення кваліфікації в Тренінговому центрі прокурорів України, доступного як онлайн на платформі дистанційного навчання [216], так і на очних тренінгах.

Таким чином, практика буквального використання слідчими та прокурорами терміна «Протокол Берклі» для позначення протоколів огляду інформації з відкритих джерел без належного розуміння змісту цього міжнародного документа засвідчує існування певного розриву між формою та сутністю відповідної слідчої дії. Це, своєю чергою, підкреслює потребу у цілеспрямованому ознайомленні з положеннями Протоколу Берклі та їх адаптації до вимог національного законодавства.

Варто проаналізувати Протокол Берклі, зосередившись на найважливіших положеннях, що можуть бути цікавими слідчим, прокурорам та суддям. Цей аналіз ґрунтуватиметься на українському перекладі Протоколу Берклі [238], який, однак, не є досконалим, тому внесемо певні зміни з огляду на оригінальний текст [318]. Розділ II Протоколу Берклі «Принципи» передбачає, що для дотримання

професійних принципів, пов'язаних із розслідуваннями з використанням цифрових даних у відкритому доступі, слідчі повинні переконатися, що вони є відповідальними, компетентними та об'єктивними, а їхня робота виконується відповідно до законодавства і з належною повагою до міркувань безпеки. Акцентується, що всі слідчі повинні керуватися етичними міркуваннями. Розділ III «Нормативно-правова база» містить визначення того, які закони застосовуються, має вирішальне значення при прийнятті рішення, що збирати, та про найкращі способи останнього. Це буде змінюватися залежно від особистості слідчих, їх цілей, мети їх розслідування та юрисдикції, в якій вони, цілі, дані та юридичні процеси, знаходяться. Збереження цифрового матеріалу має здійснюватися таким чином, щоб зберегти його автентичність та документувати ланцюг забезпечення збереження, збільшити ймовірність того, що він може бути прийнятий як доказ у суді. Розділ IV «Безпека» визначає, що кожен несе відповідальність за забезпечення безпеки розслідування та тих, на кого воно впливає, а не лише фахівці з ІТ. Міркування безпеки мають бути подвійними: (а) пов'язані з інфраструктурою, включаючи апаратне забезпечення, ПЗ та мережі; і (b) пов'язані з поведінкою, включаючи поведінку слідчих та всіх тих, з ким вони спілкуються. Оцінку безпеки слід проводити на трьох рівнях, включаючи рівень організації, конкретне розслідування/справу та конкретні заходи/завдання. У Розділі V «Підготовка» надано рекомендації щодо підготовки та стратегічного планування, що є ключем до ретельного та безпечного розслідування. Підготовка включає три процеси: (а) оцінка загроз та ризиків і опрацювання плану пом'якшення цих загроз та ризиків; (b) оцінка інформаційного ландшафту; і (c) розроблення плану розслідування [318].

Одним з найважливіших для завдань цього дослідження є Розділ VI «Процес розслідування», який окреслює основні етапи процесу розслідування та вимоги щодо його документування на кожному етапі. Цикл розслідування із використанням даних з відкритих джерел включає 6 елементів: онлайн-запити; попередня оцінка; збирання; збереження; перевірка; слідчий аналіз. У сукупності це частина циклу, який може повторюватися багато разів протягом всього

розслідування, оскільки нововідкрита інформація веде до нових напрямків дослідження.

Онлайн-запити. Є два основні процеси для онлайн-запитів: (а) пошук, тобто виявлення інформації та джерел інформації за допомогою загальних або розширених методологій пошуку; і (б) моніторинг, тобто виявлення нової інформації шляхом послідовного та наполегливого огляду набору постійних джерел (п. 141 Протоколу Берклі). Пошук або ж інтернет-пошук — це діяльність, орієнтована на виявлення нової інформації, що стосується визначеної мети або досліджуваного питання. Документація структурованих пошуків повинна містити таку інформацію: об'єктивні та дослідницькі запитання; факти, припущення та прогалини; пошукові терміни та ключові слова (доцільно створити списки ключових слів); пошукові запити та пошукові системи (мають відстежуватися та фіксуватися) (п. 142 Протоколу Берклі).

Попередня оцінка. Перш ніж збирати контент з інтернету, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні провести попередню оцінку будь-якого матеріалу, який вони ідентифікують, щоб уникнути надмірного збору та дотримання принципів мінімізації даних та цілеспрямованого розслідування, а також для забезпечення права на приватне життя приватних осіб (п. 147 Протоколу Берклі). Для визначення необхідності в збиранні цифрового елемента з мережі Інтернет повинні враховуватися такі фактори як: елегантність даних (п. 148); достовірність даних (п. 149); ризик видалення даних (п. 150); безпека (п. 151); подальші обов'язки щодо захисту даних (п. 152 Протоколу Берклі).

Збирання — це акт заволодіння інформацією в інтернеті за допомогою знімка екрана, конвертації у PDF, експертного завантаження чи іншої форми захоплення. Після того як цифровий контент буде ідентифіковано та визнано відповідним для розслідування, та *prima facie* відповідним та надійним для своєї мети, слідчий повинен визначити належний метод збору (п. 153 Протоколу Берклі).

Пункт 155 Протоколу Берклі визначає вказівки щодо того, що та як збирати. Існує кілька інструментів, які допомагають зафіксувати наведену нижче інформацію, або це можна зробити вручну. Збирання всієї наведеної нижче

інформації вважається найкращою практикою, однак перші три пункти (єдиний локатор ресурсів (URL), вихідний код мови розмітки гіпертексту (HTML) та захоплення всієї сторінки) служать мінімальним стандартом для надання доказів у суді. Звичайно, такі стандарти будуть відрізнятися в різних контекстах, але захоплення всіх перерахованих нижче елементів забезпечить сталу основу в будь-якому контексті:

а) цільова вебадреса: вебадресу зібраного контенту, також відому як єдиний локатор ресурсів (URL) або ідентифікатор (URI), слід записати;

б) вихідний код: слідчі повинні захопити вихідний код HTML вебсторінки, якщо це можливо. Вихідний код HTML містить набагато більше інформації, ніж видима частина вебсайту. Вихідний код HTML сприятиме автентифікації зібраного матеріалу;

с) захоплення всієї сторінки: слідчі повинні спочатку зробити знімок екрана цільової вебсторінки із зазначенням дати та часу. Причина цього процесу полягає в найкращому уявленні про те, що було побачено під час збору;

д) вбудовані мультимедійні файли: наприклад, якщо завантажують вебсторінку з відео або зображеннями, ці конкретні елементи також слід витягти та зібрати з вебсторінки;

е) вбудовані метадані: слідчі повинні зібрати додаткові метадані цифрового елемента, якщо вони є та застосовні. Метадані можуть змінюватися залежно від джерел, але загальні метадані включають ідентифікатор користувача завантажувача; ідентифікатор публікації, зображення чи відео; дату та час завантаження; геотег; гештег; коментарі; анотацію;

ф) контекстуальні дані: контекстний контент також слід збирати, якщо він має значення для розуміння цифрового елемента. Вони можуть включати коментарі до відео, зображення чи публікації; передбачати завантаження інформації; та/або інформацію про завантажувача/користувача, таку як ім'я користувача, справжнє ім'я чи біографію. Необхідність збору навколишньої інформації слід визначити, виходячи зі специфіки випадку та цифрового матеріалу;

g) дані збору: слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні записати всі відповідні дані, що стосуються збору, такі як ім'я збирача, IP- адреса машини, яка використовується для збору інформації, віртуальна особистість, за наявності, та мітка часу. Слідчі повинні переконатися, що системний годинник точний, бажано шляхом його синхронізації з сервером мережевого протоколу часу. Причиною цього кроку є забезпечення того, щоб метадані, пов'язані з часом, були точно представлені у зібраних файлах. Якщо для доступу до зібраної інформації використовується віртуальна особистість, це слід зазначити;

h) геш-значення – це унікальна форма цифрової ідентифікації, яка за допомогою криптографії підтверджує, що зібраний контент є унікальним і не змінювався з моменту збору. На момент збору слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні вручну додати (або інструмент збирання автоматично додати) значення гешу. Існує безліч різних типів гешів, і стандарти з часом змінилися. Слідчі повинні оцінити, який геш використовувати, виходячи з прийнятого на цей час стандарту [318].

Збереження. Постійність та доступність інформації в інтернеті часто є нестабільною (п. 157). Властивості цифрового елемента, які необхідно охороняти та зберігати з плином часу, включають його автентичність (п. 160); доступність (п. 161); ідентичність (п. 162); стійкість (п. 163); можливість відображення (п. 164); зрозумілість (п. 165). Має бути розглянуто та сплановано конкретні питання, що можуть виникнути під час пошуку даних або при їх збереженні (п. 166), зокрема: ланцюг збереження доказів (п. 167); Доказова копія – це цифровий елемент, зібраний слідчим у його первісному вигляді, який не слід змінювати (п. 168); робочі копії цифрового елемента, які слід створити для цілей аналізу та зберігати окремо, щоб слідчі могли працювати з копією, а не з оригіналом (п. 169); зберігання, що допомагає забезпечити довготривалість цифрових елементів та можливість їх пошуку та відновлення (п. 170); резервне копіювання (п. 171); погіршення якості. Якість носіїв з часом погіршується тому важливо підтримувати резервні копії та регулярно контролювати інфраструктуру зберігання і сталість збережених файлів

(п. 172); застарілість. Цифрові файли стають застарілими, коли апаратне забезпечення, необхідне для доступу до даних, більше недоступне або не може належним чином обслуговуватися (п. 173); відновлення даних. Цифрові файли можуть бути випадково або цілеспрямовано видалені (п. 174); оновлення, що передбачає копіювання контенту з одного носія інформації на інший (п. 175 Протоколу Берклі).

Перевірка належить до процесу встановлення точності чи достовірності інформації, зібраної в мережі. Перевірка інформації у відкритому доступі може бути здійснена як частина загальнодоступного аналізу – включаючи інформацію із закритих та конфіденційних джерел – або спиратися виключно на відкриті джерела (п. 176). Вона включає три складові: аналіз джерела, технічний аналіз та аналіз контенту.

Слідчий аналіз – це практика перегляду та інтерпретації фактичної інформації для опрацювання істотних висновків, що мають значення для прийняття рішень або розроблення справ. Обсяг та різна якість інформації у відкритому доступі вимагає добре структурованого підходу до аналізу (п. 195).

У Розділі VII «Звітування про висновки» йдеться про те, що результати розслідування з використанням даних у відкритому доступі, що стосуються або зібраних даних, або висновків, зроблених із цих даних, можна повідомляти усно, візуально або письмово. Слідчі повинні враховувати, які формати є найбільш прийнятними для їхніх мандатів та цільової аудиторії – беручи до уваги такі фактори, як технологічна грамотність аудиторії та доступність, об'єктивність, прозорість та безпека – при прийнятті рішення щодо (а) форматів, які будуть використовуватися, та (b) даних, які потрібно включити [238].

Пункт 208 Протоколу Берклі вказує, що звіти можуть бути призначені для внутрішнього використання або для зовнішньої публікації й розглядатися як експертні чи не експертні залежно від низки чинників [238]. Також Протоколом Берклі визначено такі форми звітності як: Письмова звітність. Письмові звіти повинні містити такі розділи: а) слідчі цілі; b) методологія; c) виконана діяльність; d) основні дані та джерела; e) прогалини або невизначеності; f) результати та

рекомендації (п. 210); Усна звітність. Що стосується судових розглядів, то часто саме керівники розслідувань мають надавати свідчення, і вони повинні мати можливість говорити про роботу своїх команд (п. 210); Візуальна звітність. Візуалізація даних – це графічне представлення інформації у вигляді, наприклад, діаграм, графіків, таблиць, карт та інфографіків, що забезпечують доступний спосіб побачити та зрозуміти тенденції, відмінні риси та закономірності у даних (п. 210). Інші види візуалізації даних включають: інтелект-карти, блок-схеми, інфографіку (п. 215 Протоколу Берклі).

Розділ VII відбиває необхідність нового, сучасного підходу до представлення результатів OSINT-розслідувань у судовому процесі. Йдеться не лише про традиційні письмові звіти, а й про використання сучасних засобів телекомунікації та мультимедійних технологій. Для кримінального процесу України це означає потребу адаптувати процесуальну практику до використання інноваційних інструментів візуалізації та забезпечити можливість безпосереднього представлення розслідувань їх авторами у залі суду, що сприятиме підвищенню доказової цінності матеріалів, зібраних з відкритих джерел.

Сам Протокол Берклі є досить об'ємним і деталізованим документом, що містить чималу кількість методологічних положень та технічних рекомендацій, які потребують глибокої фахової підготовки для належного розуміння та застосування. Для практиків кримінального процесу України його сприйняття може становити певну складність, оскільки він охоплює як правові, так і технологічні, організаційні та етичні аспекти роботи з цифровими даними. У цьому контексті доцільно звернутися й до профільної наукової літератури, яка пропонує систематизований аналіз положень Протоколу, роз'яснює їх у прикладному ключі та демонструє можливості адаптації міжнародних стандартів до національного законодавства і практики. Це дозволяє забезпечити більш цілісне розуміння документа та підвищити його ефективне використання у вітчизняному кримінальному процесі. Так, для суб'єктів кримінального провадження у контексті досліджуваного питання буде корисним підручник О. О. Торбаса «OSINT при розслідуванні кримінальних правопорушень» (2024) [273].

Розгляд змісту Протоколу Берклі засвідчує його значення як комплексного міжнародного документа, що встановлює методологічні, етичні та процесуальні стандарти роботи з інформацією з відкритих джерел у сфері кримінального правосуддя. Водночас практична його цінність проявляється не лише у положеннях Протоколу, а й у тому, наскільки активно вони впроваджуються у діяльність національних судів. Саме тому далі увагу доцільно зосередити на дослідженні судової практики, яка демонструє, яким чином українські суди, а також міжнародні судові інституції сприймають і застосовують результати OSINT-розслідувань та положення Протоколу Берклі у процесі оцінки доказів.

Протокол Берклі судовою системою України фактично вже визнаний, про що свідчить згадка про нього в постанові ККС ВС від 31.07.2024 у справі № 308/13071/22 [87], постанові ККС ВС від 27.01.2025 у справі № 947/22776/22 [87] та в численних рішеннях судів першої та апеляційної інстанцій. Про практичну проблему із належною архівацією даних, які містяться у відкритих джерелах, вже вели мову як судді ВС, вказуючи, що іноді засади безпосередності доказів, так і науковці [134; 18, с. 234-235].

Цифрові відомості все активніше інтегруються у практику доказування як на рівні національних судів, так і в юрисдикціях міжнародних судових інституцій, зокрема ЄСПЛ [332] та Міжнародного кримінального суду [241; 242]. У рішеннях ЄСПЛ вже простежується використання даних із соціальних мереж та систем обміну повідомленнями як джерела доказів, що фактично відповідають категорії матеріалів з відкритих джерел. Хоча такі відомості ще не виділялися окремо в контексті їхньої прийнятності як самостійного виду доказів, суд визнає їх потенційну значущість, проте оцінює перш за все зміст інформації, а не форму її існування.

На нашу думку, в контексті внесення змін до КПК України щодо досліджуваної категорії кримінальних процесуальних правовідносин доцільно розмежовувати таку слідчу (розшукову) дію як огляд віртуального середовища, що регламентуватиме процесуальний порядок доступу слідчого або прокурора до даних, що зберігаються у хмарних сервісах, електронних кабінетах та соціальних

мережах, та пошук відомостей у віртуальному середовищі на основі відкритих джерел інформації, що забезпечуватиме документування інформації з відкритих джерел, зокрема соціальних мереж, онлайн-платформ, супутникових карт та інших інтернет-ресурсів, однак не як одноетапної процедури, пропонованої попередньо, а як ланцюжка пошукових запитів, спрямованих на пошук інформації, що стосується обставин вчинення кримінального правопорушення. Остання повинна передбачати вимоги до протоколювання перебігу OSINT із залученням спеціаліста, фіксацію вебсторінок, скриншотів чи відеозаписів із зазначенням часу, обчислення та фіксацію геш-значень завантажуваних даних та збереження технічних параметрів середовища (IP-адрес, cookies та інших ідентифікаторів), тоді як перша, на нашу думку, могла б бути проводитися слідчим або прокурором самостійно.

Таким чином, Протокол Берклі становить собою комплексний міжнародний документ, спрямований на встановлення методологічних, етичних та процесуальних стандартів роботи з цифровою інформацією у відкритому доступі. Його застосування у кримінальному провадженні України має особливе значення з огляду на сучасні виклики, зокрема необхідність фіксації воєнних злочинів, вчинених на тимчасово окупованих територіях. Разом із тим практика показує, що використання цього документа українськими органами досудового розслідування та судами ще не стало системним, до того ж норми КПК України не містять чітких процесуальних правил роботи з інформацією з відкритих джерел. Це створює ризик невідповідності зібраних матеріалів критеріям належності та допустимості доказів.

Однак уже простежується позитивна динаміка, адже Протокол Берклі офіційно перекладено і рекомендовано до використання ОГП, його положення все частіше знаходять відображення у судових рішеннях, включно з практикою ВС. Тож він поступово стає орієнтиром у вітчизняному кримінальному процесі, хоча його потенціал реалізовано ще не повною мірою. Вказане обумовлено відсутністю в КПК України чіткого процесуального порядку роботи з цифровою інформацією з відкритих джерел. Врегулювання цього питання, зокрема шляхом запровадження нових слідчих (розшукових) дій, дозволить підвищити ефективність досудового розслідування.

4.2. Механізми Конвенції про кіберзлочинність та практика їх застосування в кримінальному процесі України

Найважливішим міжнародним документом стосовно доказів електронної форми є Конвенція про кіберзлочинність, ухвалена у 2001 році [148, с. 1]. Це перший міжнародний договір, що встановлює спільну кримінальну політику, спрямовану на захист суспільства від кіберзлочинності, а також процесуальні повноваження щодо збору доказів електронної форми механізми міжнародної співпраці в цій сфері.

Для цілей Конвенції про кіберзлочинність сформульовано визначення окремих понять (комп'ютерна система, комп'ютерні дані, постачальник послуг, дані про рух інформації), а також передбачено заходи, що мають здійснюватися на національному рівні (Розд. II), що стосуються матеріального кримінального права та процесуального права. З огляду на особливості кіберзлочинів з використанням мережі Інтернет та дистанційного запуску шкідливих програм, питанням міжнародного співробітництва присвячено окремий розділ Конвенції про кіберзлочинність (Розд. III). У ньому визначено загальні принципи міжнародного співробітництва; принципи екстрадиції; загальні принципи взаємної допомоги; процедури, пов'язані із запитами про взаємну допомогу у разі відсутності відповідних міжнародних угод [12, с. 189–190].

Конвенція про кіберзлочинність закріпила уніфіковану систему процесуальних механізмів, спрямованих на забезпечення ефективної роботи з доказами електронної форми. Як відображення сучасних викликів у сфері кримінальної юстиції, ці механізми спрямовані на досягнення ефективного кримінального переслідування щодо збирання доказів у цифровому середовищі. Тож у цьому контексті варто розглянути такі механізми: термінове збереження комп'ютерних даних, які зберігаються (ст.ст. 16, 29); термінове збереження і часткове розкриття даних про рух інформації (ст.ст. 17, 30); розпорядження про представлення даних (ст. 18); обшук і вилучення комп'ютерних даних, які зберігаються (ст. 19); збирання даних про рух інформації у режимі реального часу

(ст. 20); перехоплення змісту даних, що передаються (ст. 21); добровільне надання інформації (ст. 26); цілодобова мережа (НКП 24/7) (ст. 35).

Одним із процесуальних механізмів Конвенції про кіберзлочинність, що закріплений у ст. 16, є термінове збереження комп'ютерних даних, які зберігаються (expedited preservation of stored computer data). Його мета полягає у забезпеченні можливості збереження інформації, яка може мати значення для кримінального провадження, до моменту отримання уповноваженими органами формального доступу до неї. На практиці цей механізм часто порівнюють з умовним «заморожуванням» інформації до моменту отримання до неї офіційного доступу уповноваженими правоохоронними органами, тобто його варто розглядати як тимчасовий захід.

За змістом цієї норми, кожна держава-учасниця повинна передбачити у своєму національному законодавстві повноваження компетентних органів видавати розпорядження (ордер, наказ тощо) про негайне збереження конкретних комп'ютерних даних, що вже зберігаються у комп'ютерних системах чи на електронних носіях інформації. Особа, у власності або під контролем якої перебувають дані, яких стосується вказаний ордер, повинна була б зберігати і підтримувати цілісність таких комп'ютерних даних протягом періоду, який буде необхідним для того, щоб компетентні органи отримали дозвіл на їх розкриття. Максимальний термін такого зберігання визначено у 90 днів.

Цей механізм важливий у зв'язку з тим, що цифрові дані є вразливими до зміни, знищення чи видалення. Їх збереження вимагає оперативного, майже миттєвого, реагування, а офіційні кримінальні процесуальні процедури, зокрема міжнародна взаємодія між правоохоронними органами різних держав, може тривати довго й мати наслідком несвоєчасне втручання, що призведе до безповоротної втрати доказів електронної форми.

Водночас норми ст. 16 Конвенції про кіберзлочинність передбачають, що держава має забезпечити конфіденційність заходів зі збереження даних та недопущення розголошення факту здійснення відповідної процесуальної дії. Це пояснюється необхідністю забезпечити ефективність такого заходу у разі коли

потенційний правопорушник дізнається про зацікавленість правоохоронних органів у певних даних.

Важливо зазначити, що у ст. 16 Конвенції про кіберзлочинність встановлено лише вимогу щодо збереження даних, тоді як питання доступу до цих даних здійснюється в порядку міжнародної правової допомоги. Сам процедурний механізм реалізації термінового збереження комп'ютерних даних, які зберігаються в контексті міжнародного співробітництва під час кримінального провадження, вимоги до запитів та особливості відмови в їх виконанні передбачено в ст. 29 Конвенції про кіберзлочинність. Це підкреслює, що цей інститут не є самодостатнім інструментом, а виконує допоміжну, превентивну функцію, спрямовану на захист від втрати даних, що потенційно можуть стати доказами.

Досліджуваний механізм, передбачений ст. 16 Конвенції про кіберзлочинність, не отримав відбиття у КПК України. Вбачається, що за аналогією може застосовуватися тимчасовий доступ до речей і документів, проте повноцінний інститут термінового збереження даних у значенні, закріпленому у Конвенції про кіберзлочинність, до КПК України не інтегрований. На практиці це спричиняє ситуації, коли слідчі органи позбавлені можливості ефективно реагувати на ризик знищення або зміни інформації до моменту отримання ухвали слідчого судді.

Інститут термінового збереження комп'ютерних даних, що закріплений у ст. 16 Конвенції про кіберзлочинність, формує важливий елемент процесуального інструментарію роботи з доказами електронної форми який потребує належної імплементації в КПК України. Його впровадження дозволить забезпечити оперативне реагування на виклики, пов'язані з динамічністю цифрової інформації, та створити належні умови для збереження доказів електронної форми до моменту отримання уповноваженими органами доступу до них.

У статті 17 Конвенції про кіберзлочинність передбачено спеціальний процесуальний механізм, що є логічним продовженням положень ст. 16, а саме – термінове збереження і часткове розкриття даних про рух інформації (*expedited preservation and partial disclosure of traffic data*). Цей інструмент спрямований на

забезпечення можливості встановлення та розкриття всього маршруту передавання даних у телекомунікаційних мережах (що є ключовим для встановлення джерела, одержувача та характеру електронних комунікацій, які можуть мати значення у кримінальному провадженні), однак без розкриття змісту інформації, що передається за цим маршрутом. Тобто ця норма передбачає не лише збереження даних про рух інформації, а можливість термінового розкриття запитуючій стороні такого обсягу даних про рух інформації, що є достатньою для ідентифікації постачальників послуг і маршруту, яким була передана інформація. Таким чином може бути забезпечено оперативне встановлення місця перебування правопорушника та проведення слідчих (розшукових) дій на місці вчинення злочину. Варто також зауважити, що процедурний механізм термінового розкриття збережених даних про рух інформації в контексті міжнародного співробітництва під час кримінального провадження, зокрема особливості відмови в виконанні такого запиту, передбачено статтею 30 Конвенції про кіберзлочинність.

Згідно з цією нормою кожна держава-учасниця зобов'язана передбачити у національному законодавстві правові механізми, що дозволяють компетентним органам видавати розпорядження про термінове збереження даних про рух інформації. При цьому важливим є не лише саме збереження даних, а й можливість отримання від провайдера інформації про всі телекомунікаційні компанії чи вузли мережі, через які проходили відповідні дані. Ця вимога впливає з особливостей архітектури мережових комунікацій: дані про рух, як правило, розподілені між кількома операторами й лише комплексний доступ до них дозволяє відновити весь маршрут комунікації. У цьому сенсі ст. 17 Конвенції про кіберзлочинність виступає процесуальною гарантією того, що збереження даних про рух буде ефективним, а компетентні органи зможуть простежити повний ланцюг передавання інформації. Такий підхід унеможливорює ситуацію, коли збережені дані втрачають доказове значення через відсутність відомостей про проміжні точки маршруту.

Таким чином, ст. 17 Конвенції про кіберзлочинність формує окремий механізм, який дозволяє правоохоронним органам не лише зберегти важливі дані

про рух інформації, але й оперативно встановити повний ланцюг передавання комунікацій з одночасним забезпеченням захисту змісту даних, що передаються.

У КПК України положень, аналогічних до ст. 17 Конвенції про кіберзлочинність, у прямій формі бракує. Хоча ст. 263 КПК України встановлює порядок зняття інформації з електронних комунікаційних мереж, вона не забезпечує інституту термінового збереження та часткового розкриття даних про рух у розумінні Конвенції про кіберзлочинність. Відсутність такого інструменту ускладнює роботу слідчих та прокурорів, особливо у випадках розслідування транскордонних злочинів, коли маршрути комунікацій охоплюють кілька юрисдикцій. Щоб усунути цю нормативну прогалину, доцільно доповнити КПК України статтею 245-2 «Термінове збереження комп'ютерних даних, які зберігаються, та тимчасове розкриття даних про рух інформації».

Важливе місце у системі процесуальних механізмів Конвенції про кіберзлочинність посідає ст. 18, яка регламентує механізм production order – обов'язкового розпорядження про представлення даних. Цей інструмент забезпечує компетентним органам можливість у встановленому порядку зобов'язати провайдерів або інші суб'єкти, які володіють інформацією, надати визначені категорії даних для цілей кримінального провадження. Відповідно до змісту ст. 18 Конвенції про кіберзлочинність, держава-учасниця повинна передбачити у своєму законодавстві повноваження, що дозволяють своїм компетентним органам видавати два види ордери:

а) особам, яка знаходиться на її території – видавати ордер, що зобов'язуватиме надати зазначені в ньому комп'ютерні дані, якими така особа володіє або які контролює і які зберігаються у комп'ютерній системі або на комп'ютерному носії інформації;

б) постачальнику послуг, який пропонує свої послуги на території цієї держави – видавати ордер, що зобов'язуватиме надати інформацію про користувача послуг, інформацію, пов'язану з такими послугами, яка знаходиться у власності або під контролем цього постачальника послуг.

Застосування інституту production order має кілька суттєвих переваг. По-перше, він дозволяє уникнути більш інвазивних процесуальних заходів, таких як обшук чи вилучення комп'ютерних систем і носіїв інформації. Це відповідає принципу пропорційності у кримінальному процесі, адже обмежує втручання у сферу приватності лише до тієї міри, яка є необхідною для досягнення мети розслідування. По-друге, production order забезпечує швидкість реагування, що має вирішальне значення в умовах, коли електронні дані можуть бути знищені або змінені. По-третє, такий підхід створює процесуальну визначеність для провайдерів, які, діючи на підставі офіційного розпорядження, уникають ризиків, пов'язаних із порушенням режиму захисту персональних даних чи таємниці комунікацій.

Для кримінального процесу України імплементація ст. 18 Конвенції про кіберзлочинність має особливе значення. Чинний КПК України передбачає процедури тимчасового доступу до речей і документів (ст. ст. 159–166), проте вони не забезпечують усіх елементів, притаманних production order у розумінні Конвенції про кіберзлочинність. По-перше, у законі немає чіткого формулювання, яке б охоплювало всі категорії комп'ютерних даних, включно з інформацією про користувача послуг. По-друге, чинна редакція статей 159–165 КПК України не враховує особливостей існування документів та даних в електронній формі. Через це практична реалізація отримання доказів електронної форми ускладнюється, особливо в умовах необхідності швидкого реагування.

З метою усунення зазначених недоліків пропонуємо внести зміни до ст. 160 КПК України, передбачивши право суду за клопотанням прокурора зобов'язати будь-яку фізичну чи юридичну особу надати саме комп'ютерні дані, які перебувають у її володінні або під її контролем, а також зобов'язати постачальників електронних комунікаційних послуг надавати інформацію про користувачів таких послуг. Такий підхід відповідає змісту ст. 18 Конвенції про кіберзлочинність, де прямо визначено, що об'єктом ордера на представлення можуть бути будь-які наявні комп'ютерні дані, у тому числі відомості про користувача послуг.

У ст. 19 Конвенції про кіберзлочинність визначено основний процесуальний інструмент у сфері роботи з доказами електронної форми – обшук і вилучення комп'ютерних даних, які зберігаються (search and seizure of stored computer data). Цей інститут є одним із найбільш чутливих у контексті дотримання прав людини, оскільки пов'язаний із безпосереднім втручанням у приватне життя особи, її цифрові комунікації. Відповідно до Конвенції про кіберзлочинність кожна держава-учасниця зобов'язана надати своїм компетентним органам повноваження здійснювати обшук або подібний доступ до комп'ютерних систем і носіїв інформації з метою виявлення даних, що мають значення для кримінального провадження.

Особливе значення мають положення ч. 2 ст. 19, які закріплюють інститут так званого «розширеного обшуку». Йдеться про право компетентних органів поширювати обшук і доступ не лише на ту комп'ютерну систему, яка є об'єктом первинного втручання, але й на інші системи, що функціонально чи технічно пов'язані з нею і знаходяться у межах тієї ж юрисдикції. Цей підхід враховує специфіку мережевих технологій, у яких дані можуть бути розподілені між різними пристроями, серверами або хмарними сервісами, і лише доступ до всього комплексу пов'язаних систем дозволяє отримати повний доступ до даних, а отже й до доказів електронної форми.

Окрім самого факту доступу до даних також має бути надано повноваження компетентним органам щодо: можливості вилучення комп'ютерної системи чи її частини або електронного носія інформації; копіювання і збереження копії комп'ютерних даних; збереження цілісності комп'ютерних даних; обмеження доступу або видалення визначених комп'ютерних даних з комп'ютерної системи, до якої було отримано доступ.

Таким чином, ст. 19 Конвенції про кіберзлочинність закріплює комплексний інструментарій, що дозволяє не лише здійснювати традиційний обшук комп'ютерних систем, але й адаптувати цю процесуальну дію до особливостей цифрового середовища. Її значення полягає у поєднанні двох складових –

ефективності збирання доказів і захисту їхньої цілісності, що є важливим для подальшого використання під час судового розгляду.

В українському кримінальному процесі вимоги щодо обшуку та вилучення комп'ютерних даних частково відображено у КПК України. Ба більше, в абз. 2 ч. 6 ст. 236 КПК України відображено процедури проведення «розширеного обшуку», що, на нашу думку, імплементує норми ч. 2 ст. 19 Конвенції про кіберзлочинність. Однак наявні інструменти обшуку, арешту майна або тимчасового доступу до речей і документів не повністю охоплюють специфіку електронних даних, які можуть бути змінені чи видалені дистанційно у будь-який момент. Тому імплементація положень ст. 19 Конвенції про кіберзлочинність потребує запровадження у КПК України спеціальних норм.

Статтею 20 Конвенції про кіберзлочинність закріплено один із найбільш технічно складних і водночас стратегічно важливих механізмів – збирання даних про рух інформації у режимі реального часу (real-time collection of traffic data). На відміну від інституту термінового збереження (ст.ст. 16–17), який має на меті зберегти вже наявні дані, ст. 20 передбачає можливість збирання даних про рух інформації у момент її передавання телекомунікаційними мережами. Зміст норми полягає у тому, що кожна держава-учасниця повинна передбачити у своєму законодавстві повноваження компетентних органів самостійно збирати й записувати технічними засобами дані про рух інформації у режимі реального часу, а також зобов'язувати провайдерів телекомунікаційних послуг здійснювати збір і фіксацію таких даних, співпрацювати з компетентними органами в цій діяльності. Йдеться не про зміст електронних повідомлень, а саме про їх технічні характеристики: маршрут, тривалість, час відправлення та отримання, IP-адреси відправника й одержувача, використані порти тощо. Ці дані є надзвичайно важливими для встановлення зв'язків між учасниками комунікацій, виявлення структури злочинних мереж та ідентифікації осіб, які перебувають «за екраном» комп'ютерних систем.

Правова природа ст. 20 Конвенції про кіберзлочинність свідчить про поєднання двох ключових цілей: оперативне документування комунікацій у

динамічному цифровому середовищі; забезпечення дотримання прав людини, адже збір даних про рух інформації обмежує приватність значно менше, ніж перехоплення змісту повідомлень (ст. 21).

Для українського кримінального процесу ця норма має особливе значення, позаяк вітчизняне законодавство лише частково охоплює відповідний інструментарій. Так, ст. 263 КПК України встановлює процедуру зняття інформації з електронних комунікаційних мереж, яка може застосовуватися і до даних про рух. Проте ця норма не містить чіткої регламентації саме збирання даних у реальному часі в розумінні Конвенції про кіберзлочинність, що створює правову невизначеність у практиці правозастосування. Доцільно переглянути зміст ст. 263 КПК України з тим, щоб чітко розмежовувати доступ до змісту інформації та до даних про рух інформації. Перший із зазначених видів доступу є більш інвазивним і може здійснюватися виключно за ухвалою слідчого судді за наявності обґрунтованої підозри у вчиненні тяжкого чи особливо тяжкого злочину або злочину. Такий підхід відповідає міжнародним стандартам і спрямований на забезпечення пропорційності втручання.

Слід підкреслити, що ст. 20 Конвенції про кіберзлочинність є проявом тенденції до мінімізації втручання при одночасному забезпеченні ефективності доказування. Дані про рух інформації не розкривають змісту комунікацій, але надають слідству можливість вибудувати картину взаємодії між особами та встановити ключові вузли злочинної діяльності.

Стаття 21 Конвенції про кіберзлочинність закріплює один із найбільш чутливих та інвазивних процесуальних інструментів – перехоплення змісту даних, що передаються (*interception of content data*). На відміну від ст. 20, яка стосується збирання лише даних про рух інформації, ст. 21 стосується безпосередньо змісту комунікацій – текстових повідомлень, голосових розмов, переданих файлів, відео та аудіо, тобто тієї інформації, яка складає сутність приватної комунікації.

Держави-учасниці зобов'язані передбачити у національному законодавстві можливість для компетентних органів здійснювати перехоплення змісту даних у режимі реального часу. Це може відбуватися як за допомогою використання

компетентними органами спеціальних технічних засобів, так і шляхом зобов'язання провайдерів телекомунікаційних послуг забезпечувати правоохоронним органам сприяти у здійсненні такого перехоплення. При цьому має бути забезпечено законодавчі та інші заходи, щоб зобов'язати провайдерів телекомунікаційних послуг зберігати конфіденційність факту здійснення перехоплення.

У кримінальному процесуальному законодавстві України найближчим аналогом до ст. 21 Конвенції про кіберзлочинність є такий вид НСРД, як зняття інформації з електронних комунікаційних мереж (ст. 263 КПК України). Втім, слід зазначити, що чинні положення КПК України не містять достатньо чіткої регламентації саме інституту перехоплення змісту даних, що передаються, у контексті міжнародних стандартів. Відсутність деталізованих норм щодо гарантій пропорційності та контролю може створювати ризики як для правозастосовної практики, так і для захисту прав людини. З огляду на це, постає необхідність оновлення понять, що стосуються процесуальних гарантій у цьому контексті.

Не менш важливим є технологічний вимір імплементації ст. 21 Конвенції про кіберзлочинність. Реалізація перехоплення змісту даних, що передаються, вимагає від провайдерів телекомунікаційних послуг наявності технічних рішень, що здатні забезпечити безперервний та захищений доступ до каналів комунікації. Водночас держава повинна встановити правові механізми контролю за використанням таких технічних засобів, аби запобігти їх неправомірному застосуванню, витоку даних або несанкціонованому втручання третіх осіб. У цьому контексті постає завдання гармонізації процесуальних норм із вимогами інформаційної безпеки та забезпечення ефективного кіберзахисту, що особливо актуально для України з огляду на підвищений рівень кіберзагроз.

У ст. 26 Конвенції про кіберзлочинність визначено механізм, який має суттєве значення у сфері міжнародного співробітництва, – добровільне надання інформації. На відміну від інших інститутів, що ґрунтуються на офіційних запитах чи формалізованих процедурах взаємної правової допомоги, цей механізм передбачає можливість компетентних органів однієї держави самотійно

передавати інформацію іншим державам-учасникам без попереднього їх звернення. Зміст цієї норми полягає у тому, що якщо органи влади однієї держави отримали у процесі розслідування дані, які можуть становити інтерес для іншої держави у зв'язку з розслідуванням злочину, вони мають право за власною ініціативою надіслати такі відомості без формального запиту. Це положення можна розглядати як прояв активного сприяння міжнародному співробітництву у сфері боротьби з кіберзлочинністю.

Особливе значення цього інституту полягає у його оперативності. На відміну від класичної моделі міжнародної правової допомоги, яка є процедурно складною та досить тривалою, добровільне надання інформації дозволяє швидко обмінюватися доказами електронної форми та оперативно реагувати на виклики, пов'язані з кіберзлочинністю. Цей механізм фактично трансформує традиційний підхід, за якого міжнародне співробітництво обмежувалося суворою формалізацією. Відтепер акцент робиться на гнучких, динамічних механізмах, які враховують специфіку кіберпростору та швидкоплинність доказів електронної форми.

Важливо звернути увагу, що згідно з положеннями ч. 2 ст. 26 Конвенції про кіберзлочинність сторона, яка надає інформацію, перш ніж її надавати, може вимагати, щоб вона залишалася конфіденційною або використовувалася за певних умов. Якщо сторона, яка отримує інформацію, не може задовольнити заявлені вимоги, то про це має бути повідомлено. Таким чином, сторона, яка надає інформацію, вже після цього визначає, надавати інформацію, чи ні. Якщо ж сторона, яка отримує інформацію, приймає її за певних умов, вона має їх дотримуватися.

Добровільне надання інформації тісно пов'язане з довірою держав-учасниць до процесуальних інститутів одна одної. Його застосування можливе лише за умови взаємного встановлення і визнання належного рівня захисту прав людини, ефективної антикорупційної політики, процесуальних гарантій та дотримання стандартів поведінки з доказами електронної форми в тому числі забезпечення безпеки їх зберігання та контролю доступу.

У контексті кримінального процесу України цей механізм потребує чіткої інтеграції у національне законодавство. Наразі ст. 541 КПК України визначає поняття «запитуюча сторона» та «запитувана сторона», однак немає «передаюча сторона» (або його аналог) у значенні, яке використовується у ст. 26 Конвенції про кіберзлочинність. А це ускладнює повноцінне застосування інституту добровільного надання інформації. Тому варто розглянути можливість доповнення КПК України такою дефініцією, яка б закріпила право держави не лише відповідати на запити, а й передавати дані з власної ініціативи у випадках, коли це об'єктивно сприятиме розслідуванню.

Таким чином, ст. 26 Конвенції про кіберзлочинність виступає важливим інструментом, що дозволяє державам-учасницям оперативно реагувати на кіберзлочини, не чекаючи формальних запитів. Для кримінального процесу України імплементація цього положення означатиме підвищення ефективності міжнародного співробітництва, створення правових підстав для становлення проактивної позиції у питаннях передачі доказів електронної форми.

У ст. 35 Конвенції про кіберзлочинність передбачено створення цілодобової мережі національних контактних пунктів (Національний контактний пункт 24/7, НКП 24/7), що працюють цілодобово та забезпечують оперативну взаємодію компетентних органів держав-учасниць у питаннях : (а) надання технічних порад; (б) збереження даних відповідно до статей 29 і 30 Конвенції про кіберзлочинність; та (с) збирання доказів, надання юридичної інформації та встановлення місцеперебування підозрюваних. Даний інструмент визнано одним із найбільш ефективних у практиці транскордонного співробітництва, адже він дозволяє у максимально короткі строки ініціювати та реалізувати процедури термінового збереження комп'ютерних даних, які зберігаються (ст. ст. 16, 29) та термінового збереження і часткового розкриття даних про рух інформації (ст. ст. 17, 30), що дозволяє зберегти ці дані до моменту надходження офіційного запиту про міжнародну правову допомогу.

У Законі України «Про ратифікацію Конвенції про кіберзлочинність» визначено, що органом, на який покладаються повноваження щодо створення та

функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є МВС України [234, с. 1]. На виконання доручення Президента України від 03.12.2010 р. № 02/78475-01 було створено контактний пункт з реагування на кіберзлочини, який увійшов до структури Департаменту боротьби з кіберзлочинністю і торгівлею людьми МВС України [12, с. 190]. На підставі Постанови Кабінету Міністрів України від 13.10.2015 р. № 831 утворено Департамент кіберполіції як міжрегіональний територіальний орган Національної поліції [236, с. 1]. Наразі Департамент кіберполіції Національної поліції України здійснює функції НКП 24/7 в Україні.

Система процесуальних механізмів, передбачених Конвенції про кіберзлочинність, формує комплексну основу для роботи з доказами електронної форми. Її ключовими елементами є оперативність, технологічна адекватність та поєднання ефективності кримінального переслідування з гарантіями дотримання прав і свобод людини. Однак розвиток технологій та глобалізаційні процеси потребують постійного вдосконалення процесуальних механізмів у досліджуваний сфері.

Саме Другий додатковий протокол до Конвенції про кіберзлочинність щодо посилення співпраці та розкриття доказів електронної форми (2021) [366] (далі – Другий додатковий протокол), присвячений посиленню співробітництва та розкриттю доказів електронної форми містить нові положення щодо: прямого звернення правоохоронних органів до провайдерів за межами юрисдикції; процедур автентифікації та захисту персональних даних; стандартів безпеки при транскордонному доступі до інформації. Другий додатковий протокол спрямований на вирішення низки питань, зокрема: 1) як домогтися більш ефективного використання облікового запису або інтернет-протоколу, який використовується для вчинення злочину; 2) як та на яких умовах здійснювати співробітництво з постачальником послуг, який перебуває на території іншої держави, для одержання доказів електронної форми; 3) як без зволікань домогтися

розкриття даних, включаючи дані про зміст, від іншої держави в надзвичайних ситуаціях; 4) як зробити міжнародне співробітництво більш ефективним та чи можна надати правоохоронним органам додаткові інструменти для збору доказів електронної форми. Підставами для прийняття Другого додаткового протоколу стали: зростання випадків використання інформаційно-комунікаційних технологій, включаючи інтернет-послуги, зростання кіберзлочинності, що ставить під загрозу демократію та верховенство права; збільшення кількості потерпілих від кіберзлочинів та важливість забезпечення правосуддя для захисту прав потерпілих; обов'язок держави нести відповідальність за захист суспільства та фізичних осіб не тільки в реальному світі, але й в інтернеті, у тому числі шляхом ефективного розслідування кіберзлочинів та судового провадження; докази злочину зберігаються в електронній формі в комп'ютерних системах, які перебувають під юрисдикцією іноземних, досить часто декількох держав [12, с. 190].

Аналіз Другого додаткового протоколу дає підстави твердити, що ним створено правову основу для прямого співробітництва з постачальниками послуг (ст.ст. 6, 7), прискорених форм співробітництва для розкриття інформації про абонента та дані трафіку (ст. 8), прискореного співробітництва та розкриття інформації у надзвичайних ситуаціях (ст.ст. 9, 10), передбачені додаткові інструменти взаємної допомоги (ст.ст. 11, 12), захист даних та інші гарантії верховенства права (ст. ст. 13, 14) [12, с. 190–191].

Прийняття Другого додаткового протоколу до Конвенції про кіберзлочинність стало черговим кроком у напрямі поглиблення міжнародного співробітництва у сфері боротьби з кіберзлочинністю та збирання доказів електронної форми. Основна його мета полягає у створенні додаткових інструментів взаємодії, спрямованих на підвищення ефективності як традиційної взаємної правової допомоги, так і сучасних форм міжнародного співробітництва між компетентними органами. Такий підхід суттєво розширює можливості використання передбачених Конвенції про кіберзлочинність механізмів, адже вони поширюються на будь-які кримінальні провадження, у яких об'єктом доказування виступають цифрові дані. Це зумовлює необхідність внесення змін до

національного кримінального процесуального законодавства з метою унормування відповідних інститутів як загальних правил збирання доказів у кримінальному процесі.

Важливим нововведенням є закріплення у Другому додатковому протоколі низки нових понять. Зокрема, «надзвичайна ситуація» визначається як обставина, що створює значний та неминучий ризик для життя або безпеки будь-якої фізичної особи; «персональні дані» трактується як будь-яка інформація, що стосується ідентифікації особи; «передаюча сторона» – держава, яка надає дані у відповідь на запит, у рамках спільної слідчої групи чи з власної ініціативи.

Значну увагу у Другому додатковому протоколі приділено питанням прямого співробітництва з постачальниками послуг, що перебувають на території інших держав. Зокрема, передбачено можливість направлення компетентними органами запитів до організацій, які здійснюють реєстрацію доменних імен, з метою отримання інформації для ідентифікації власників таких доменів. Аналогічно унормовано порядок видачі розпоряджень про надання даних про абонента, які надсилаються безпосередньо іноземному постачальнику послуг.

Новелою виступає також можливість прискореного отримання даних про абонента та технічних параметрів трафіку відповідно до ст. 8 Другого додаткового протоколу. Такий механізм передбачає обов'язок держав забезпечити наявність у компетентних органів правових підстав для вимагання від постачальників послуг, що знаходяться в іноземних юрисдикціях, розкриття збережених даних у встановлені скорочені строки.

Особливу увагу слід звернути на інститут отримання даних у надзвичайних ситуаціях (ст. 9 Другого додаткового протоколу). У такому випадку НКП 24/7 (ст. 35 Конвенції про кіберзлочинність) уповноважуються забезпечувати негайне передання запитів, що дозволяє оперативно розкривати та використовувати інформацію, необхідну для запобігання реальній загрозі життю чи безпеці особи.

Другий додатковий протокол також розширює інструментарій міжнародного співробітництва шляхом унормування проведення відео- та аудіоконференцій для

отримання показань свідків чи експертів, створення спільних слідчих груп та забезпечення їх ефективної роботи.

Таким чином, Другий додатковий протокол істотно розширює функціональні можливості держав у сфері розслідування злочинів, пов'язаних з електронними доказами, водночас закладаючи необхідність адаптації національного процесуального законодавства. Для України це означає не лише приведення положень КПК України у відповідність до міжнародних стандартів, а й формування нової доктрини збирання, використання та захисту доказів електронної форми у кримінальному провадженні.

На нашу думку, процес імплементації положень Конвенції про кіберзлочинність доцільно відокремлювати від процесу імплементації Другого додаткового протоколу, оскільки йдеться про різні за рівнем та обсягом міжнародно-правові інструменти. Водночас ці два документи перебувають у тісній взаємозалежності, формуючи взаємодоповнювальну систему стандартів у сфері збору та використання доказів електронної форми. Тому оптимальним підходом є їх розгляд та впровадження як єдиного пакета правових норм, що забезпечує комплексність і внутрішню узгодженість кримінального процесуального регулювання. В іншому разі існує ризик обмежитися фрагментарною імплементацією, яка послабить ефективність як самої Конвенції про кіберзлочинність, так і її Другого додаткового протоколу.

З урахуванням змін, внесених до КПК України у березні 2022 року щодо процесуального статусу доказів електронної форми а також їх кореляції із положеннями Конвенції про кіберзлочинність, можемо стверджувати, що Україна вживає заходів до впровадження стандартів Конвенції про кіберзлочинність. Водночас зберігаються важливі застереження, які стосуються належного визначення категорій даних, процедур їх збереження та розкриття, а також гарантій та запобіжних заходів.

Слід вказати однак, що йде системна робота щодо вдосконалення законодавства в цьому напрямі. Так, учасники Круглого столу з питань

електронних доказів у кримінальному процесі України, що відбувся 28-29 січня 2025 року у Києві, у підсумку виробили такі пропозиції:

1. Ініціювати питання щодо внесення змін до КПК України в частині:

а) імплементації інструментів Конвенції про кіберзлочинність (зокрема шляхом запровадження нових заходів забезпечення кримінального провадження щодо термінового збереження даних та ін.);

б) унормування питання фіксації, зберігання та використання під час кримінального провадження доказів електронної форми.

2. Удосконалити порядок взаємодії з НКП 24/7, що передбачає:

а) створення для слідчих, детективів та прокурорів короткого роз'яснення (one-pager) щодо існування НКП 24/7 на базі Національної поліції України, до якого включити таку інформацію: основні функції; контактна інформація та порядок взаємодії з НКП 24/7; основні шаблони запитів, що можуть бути використані для направлення цих запитів. Ці шаблони доступні на сайті Ради Європи (Preservation request, Information disclosure request); практичні рекомендації щодо заповнення існуючих форм відповідно до кожного окремого виду запиту;

б) створення та затвердження (органами досудового розслідування, ОГП та Міністерством юстиції України) міжвідомчої інструкції щодо порядку взаємодії органів досудового розслідування та органів прокуратури з НКП 24/7 (за аналогією з Інструкцією про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол [229, с. 1]). У цій інструкції пропонується, серед іншого, зобов'язати суб'єкта, який скерував запит до НКП 24/7, скеровувати запит про міжнародну правову допомогу щодо витребування збережених даних або своєчасно інформувати про відсутність потреби в подальшому зберіганні даних (див. Додаток 3);

с) проведення для слідчих, детективів та прокурорів тренінгів з юридичного письма щодо складання запитів до НКП 24/7 та запитів про міжнародну правову допомогу для зменшення термінів їх погодження та усунення причин повернення на доопрацювання (наприклад, Національною академією внутрішніх справ та Тренінговим центром прокурорів України).

Ці пропозиції знайшли підтримку також учасників Круглого столу з питань допустимості, обробки та збереження електронних доказів у кримінальному провадженні в Україні, що відбувся 11–12 червня 2025 року у Львові, організованого у співпраці з національними академічними та дослідницькими організаціями за підтримки проєкту «CyberUA: Strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine» Ради Європи.

Узагальнюючи наведене, можна стверджувати, що подальший розвиток кримінального процесуального законодавства України має відбуватися шляхом системного вдосконалення та гармонізації із положеннями Конвенції про кіберзлочинність та Другого додаткового протоколу до неї. Запровадження механізмів термінового збереження даних, унормування порядку їх фіксації та використання у кримінальному провадженні, а також удосконалення процедур взаємодії з НКП 24/7 повинні розглядатися як частина єдиного пакета правових змін. Такий підхід дозволить уникнути фрагментарності імплементації та забезпечить комплексне наближення національного процесуального законодавства до міжнародних стандартів, водночас створивши дієві гарантії для ефективного збирання та використання доказів електронної форми з урахуванням балансу між потребами кримінального переслідування і захистом прав людини.

Конвенція про кіберзлочинність залишається універсальною моделлю, що задає глобальні орієнтири для правових систем держав. Для України актуальним є не лише формальне приєднання до цих стандартів, а і їх системна інтеграція в кримінальний процес, що потребує науково обґрунтованих змін. Таким чином, імплементація у національне законодавство положень Конвенції про кіберзлочинність та Другого додаткового протоколу є необхідною умовою для підвищення ефективності доказування у кримінальних провадженнях, пов'язаних із використанням доказів електронної форми.

4.3. Практика впровадження стандарту ISO/IEC 27037:2012 в державах Європи та в Україні

Наявність стратегічно та організаційно коректного порядку роботи з доказами електронної форми під час кримінального провадження є передумовою їх результативного використання під час доказування. В умовах відсутності в КПК України норм, що забезпечують технічні аспекти ідентифікації, збирання, здобуття, збереження доказів електронної форми незамінним для правоохоронців стає ДСТУ ISO/IEC 27037:2017 [83, с. 1–31], що встановлює відповідне регулювання.

ISO/IEC 27037:2012 «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence» є спільною розробкою Міжнародної організації зі стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC). Він підготовлений Спільним технічним комітетом ISO/IEC JTC 1, Інформаційні технології, Підкомітетом SC 27, Техніки безпеки ІТ та прийнятий у 2012 році шляхом офіційного голосування їхніх національних органів-членів. Цей міжнародний стандарт містить рекомендації щодо конкретних дій при роботі з цифровими доказами, а саме: ідентифікації, збирання, придбання та збереження цифрових доказів, які можуть мати доказову цінність, а також рекомендації для осіб щодо типових ситуацій, що виникають у процесі роботи з цифровими доказами, та допомагає організаціям у дисциплінарних процедурах і сприяє обміну потенційними цифровими доказами між юрисдикціями [429].

Європейська стандартизація організовується зацікавленими сторонами та для них на основі національного представництва (Європейський комітет зі стандартизації (the European Committee for Standardisation, CEN) та Європейський комітет зі стандартизації в галузі електротехніки (the European Committee for Electrotechnical Standardisation, Cenelec)) та прямої участі (Європейський інститут стандартів телекомунікацій (the European Telecommunications Standards Institute, ETSI)), і базується на принципах, визнаних Світовою організацією торгівлі (the World Trade Organisation, WTO) у сфері стандартизації [491, с. 1].

Текст ISO/IEC 27037:2012 був схвалений CEN як EN ISO/IEC 27037:2016 без будь-яких змін. EN ISO/IEC 27037:2016 є європейським стандартом, якому надано статус національного стандарту шляхом публікації ідентичного тексту або шляхом схвалення не пізніше лютого 2017 року, а суперечливі національні стандарти мають бути відкликані не пізніше лютого 2017 року. Згідно з Внутрішнім регламентом CEN-CENELEC національні організації зі стандартизації таких країн зобов'язані впровадити цей європейський стандарт: Австрія, Бельгія, Болгарія, Хорватія, Кіпр, Чеська Республіка, Данія, Естонія, Фінляндія, Колишня Югославська Республіка Македонія, Франція, Німеччина, Греція, Угорщина, Ісландія, Ірландія, Італія, Латвія, Литва, Люксембург, Мальта, Нідерланди, Норвегія, Польща, Португалія, Румунія, Словаччина, Словенія, Іспанія, Швеція, Швейцарія, Туреччина та Велика Британія [390, с. 1].

Отож, ISO/IEC 27037:2012 системно впроваджено в державах Європи. Наприклад, BS EN ISO/IEC 27037:2016 – британський стандарт, що точно відповідає тексту ISO/IEC 27037:2012 [323]. UNE EN ISO/IEC 27037:2016 — ратифікований іспанським органом AENOR у грудні 2016 р., є точним перекладом ISO/IEC 27037:2012 [520]. SIST EN ISO/IEC 27037:2017 — словенський стандарт, повністю ідентичний EN ISO/IEC 27037:2016 [502]. CEI UNI EN ISO/IEC 27037:2017 — італійський стандарт відповідає EN ISO/IEC 27037:2016 [390]. EVS EN ISO/IEC 27037:2016 — естонський стандарт, прийнятий на основі EN ISO/IEC 27037:2016 [400] тощо.

Таким чином, впровадження ISO/IEC 27037:2012 в Європі відбулося через прийняття його як європейського стандарту EN ISO/IEC 27037:2016, який потім інтегрувався в національні системи стандартизації.

З 1 січня 2019 року в Україні набрав чинності Національний стандарт ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», прийнятий методом перекладу, — ідентичний щодо ISO/IEC 27037:2012 «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence» [83, с. 1–31]. Його

розроблено Технічним комітетом стандартизації «Банківські та фінансові системи і технології», прийнято та надано чинності наказом Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ») від 6 грудня 2017 р. № 400. Національний стандарт відповідає ISO/IEC 27037:2012 та має ступінь відповідності — ідентичний (IDT). Його розроблено згідно з правилами, установленими в національній стандартизації України на заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT) [83, с. II].

ДСТУ ISO/IEC 27037:2017 надає настанови для специфічної діяльності з оброблення потенційних доказів електронної форми такими процесами є: ідентифікація, збирання, здобуття та збереження. Ці процеси потрібні під час досудового розслідування для підтримання цілісності доказів електронної форми і становлять прийнятну методологію отримання, яка буде забезпечувати їхню допустимість у законодавчих та дисциплінарних судових процесах, а також інших потрібних інстанціях. ДСТУ ISO/IEC 27037:2017 також надає загальні настанови стосовно збирання нецифрових доказів, які можуть бути корисними на стадії аналізування потенційних доказів електронної форми. ДСТУ ISO/IEC 27037:2017 також спрямований на інформування осіб, які приймають рішення, та тих, кому потрібно визначати надійність наданих їм потенційних доказів електронної форми. Він важливий для організацій, яким необхідно захищати, аналізувати та презентувати потенційні докази електронної форми для поліцейських підрозділів, які формують та запроваджують процедури щодо доказів електронної форми часто як частину доказів більшого діапазону. Запровадження ДСТУ ISO/IEC 27037:2017 потребує відповідності національним законам, правилам та нормативним документам. Він не є заміною специфічних законодавчих вимог. Фактично, він може слугувати практичною настановою для DEFR, та фахівця з цифрової криміналістики або Digital Evidence Specialist (далі – DES) [83, с. v -vi].

Важливо зауважити, що отримати доступ до офіційного тексту ДСТУ ISO/IEC 27037:2017 [83] є складним завданням з огляду на те, що стандарти ISO є об'єктами авторського права. Національний орган стандартизації ДП «УкрНДНЦ»

забезпечує можливість придбання ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) та ДСТУ EN ISO/IEC 27037:2022 (EN ISO/IEC 27037:2016, IDT; ISO/IEC 27037:2012, IDT) на комерційній основі. Звісно, офіційні тексти міжнародних стандартів ISO розповсюджуються відповідно до Політики розповсюдження публікацій та захисту авторського права ISO – ISO POCOSA 2017. Особливості розповсюдження стандартів ISO та забезпечення технічних комітетів: стандарти ISO розповсюджуються в електронному та паперовому вигляді з нанесенням водяного знаку; ціна на офіційні тексти міжнародних стандартів ISO у паперовому та електронному вигляді однакова та встановлюється відповідно до рекомендованої ціни ISO; національні стандарти, прийняті методом підтвердження, розповсюджуються також відповідно до рекомендованої ціни ISO; ТК для розроблення національних нормативних документів забезпечуються стандартами ISO на безплатній основі, як в паперовому, так і електронному вигляді.

За інформацією ДП "УкрНДНЦ", існує можливість безплатно ознайомитись із текстами будь-яких стандартів, каталогів та класифікаторів, наявних у Національному фонді нормативних документів, у читальній залі фонду за адресою: м. Київ вул. Святошинська, 2, к. 307. Орган державної влади, зокрема правоохоронні органи, можуть звернутися з офіційним запитом до ДП «УкрНДНЦ». Запит повинен містити обґрунтування необхідності отримання ДСТУ ISO/IEC 27037:2017, а саме – використання працівниками під час роботи з доказами електронної форми.

Також доступні класичні шляхи пошуку інформації, наприклад, через звернення до Національної бібліотеки України імені В. І. Вернадського. Отримати доступ до досліджуваного ДСТУ можна як шляхом користування документними фондами НБУВ у читальних залах, так і за допомогою послуги електронного доставляння документів.

Оскільки, як зазначалось попередньо, на ДСТУ ISO/IEC 27037:2017 розповсюджуються вимоги Політики розповсюдження публікацій та захисту авторського права ISO – ISO POCOSA 2017, його публікація як додатка до цієї монографії неможлива. Однак надзвичайно актуальним є аналіз ДСТУ ISO/IEC

27037:2017 у контексті положень КПК України та практики правозастосування з огляду на таке. У вступній частині до ДСТУ ISO/IEC 27037:2017 зазначено, що документ прийнято методом перекладу [83, с. v], тобто шляхом перекладу англomовного тексту ISO/IEC 27037:2012, IDT українською мовою. Тож йде мова про прямий (в окремих положеннях навіть технічний) переклад міжнародного стандарту, що не містить посилань на КПК України або ж адаптованої термінології.

Для зручності ключові положення ДСТУ ISO/IEC 27037:2017 проаналізовано шляхом: послідовного викладу відомостей відповідно до структури досліджуваного ДСТУ; окремі пункти ДСТУ цитуємо у версії технічного перекладу українською мовою, однак в коментарях застосовуємо авторську термінологію дослідження; окремі терміни дублюємо англійською мовою відповідно до оригінального тексту ISO/IEC 27037:2012 з метою забезпечення точності передання термінології; нумеровану структуру ДСТУ диференціюємо на розділи (нумерація «1», «2» і т. д.), пункти (нумерація «6.1», «6.2» і т. д.) та підпункти (нумерація «5.3.5», «6.2.1» і т. д.) для зручності викладу.

Варто акцентувати, що ДСТУ ISO/IEC 27037:2017 є доволі складним для розуміння, тому потребує детального коментування, принаймні тієї його частини, що дозволить відобразити обсяг дисертаційного дослідження.

Розділ 1 ДСТУ ISO/IEC 27037:2017 окреслює сферу його застосування, фокусуючись на базових етапах оброблення цифрової інформації, що потенційно може бути використана як доказ. У науково-практичному аспекті важливо, що стандарт не обмежується технічними процедурами, а має міждисциплінарну спрямованість — він сприяє узгодженню підходів спеціалістів з різних юрисдикцій, що є особливо актуальним для міжнародного кримінального співробітництва під час кримінального провадження та визнання допустимими доказів, здобутих за межами України.

У контексті кримінального процесу України це положення дає змогу ідентифікувати об'єктивну потребу в розробленні для суб'єктів кримінального процесу СОП щодо роботи з доказами електронної форми, з урахуванням характеру носія та способу фіксації інформації. У законодавстві таких підходів

бракує, зокрема відсутнє нормативне розмежування між ідентифікацією, збиранням і здобуттям даних, що ускладнює практику підтвердження цілісності та автентичності таких доказів.

Окрему наукову значущість становить наведений у стандарті (хоч і не вичерпний) перелік пристроїв, який підтверджує технологічну складність об'єкта доказування. Це дає підстави для формування класифікаційних підходів до технічних джерел досліджуваної категорії доказів, а також для уточнення поняття «носії інформації» у межах ст. 99 КПК України.

Розділ 2 ДСТУ ISO/IEC 27037:2017, орієнтуючи користувача на взаємопов'язаний комплекс міжнародних стандартів, що регламентують суміжні аспекти цифрової складової доказування. У науково-практичному вимірі це дозволяє зробити кілька важливих висновків.

По-перше, включення ISO/TR 15801 свідчить про акцент на забезпеченні автентичності та надійності електронної інформації. Ці категорії є ключовими для доказування, оскільки саме достовірність і незмінність даних визначають їх допустимість та переконливість для суду. У контексті КПК України це безпосередньо співвідноситься з вимогами щодо допустимості доказів (ст. 86 КПК України). Отже, цей стандарт є важливим орієнтиром при оцінці, чи відповідає зібрана інформація таким критеріям.

По-друге, вказівка на ISO/IEC 17020 та ISO/IEC 17025:2005 акцентує на потребі у стандартизованій інституційній спроможності органів, які здійснюють інспектування або криміналістичні дослідження доказів електронної форми. Це має принципове значення для кримінального процесу в частині залучення спеціалістів та експертів (статті 69, 71, 101 КПК України), а також оцінки отриманих результатів, зокрема висновку експерта. Без дотримання відповідних стандартів якості й компетентності результати експертних досліджень цифрових слідів можуть бути поставлені під сумнів.

По-третє, ISO/IEC 27000 є концептуальним для формування термінологічного і методологічного базису у сфері інформаційної безпеки. У сфері кримінального процесу це має значення для визначення меж доступу до

інформаційних систем, фіксації слідів втручання, а також для збереження цілісності даних під час вилучення та подальшого дослідження.

Варто зазначити, що імплементація наведених стандартів у правозастосовну діяльність вимагає не лише технічної адаптації, а й процесуальної легітимації — через внесення до методик експертного дослідження, внутрішніх регламентів правоохоронних органів, методик проведення слідчих дій тощо. Їх застосування також є доцільним при розроблюванні для суб'єктів кримінального процесу СОП щодо роботи з доказами електронної форми.

Розділ 3 ДСТУ ISO/IEC 27037:2017 виконує надзвичайно важливу функцію в стандартизації базових понять, без яких неможливе ані ефективне правозастосування, ані коректне наукове осмислення процесів, пов'язаних з обробленням доказів електронної форми. У цьому коментарі подано науково-практичний аналіз значущих термінів із фокусом на їх правове значення у сфері кримінального процесу.

По-перше, важливим є розмежування понять ідентифікації, збирання, здобуття, утворення образу та збереження. У КПК України такі дії не мають чіткої легалізації, що призводить до практичних ускладнень у трактуванні моменту виникнення доказу, встановлення відповідального суб'єкта, фіксації його повноважень і дотримання ланцюга збереження доказів (*chain of custody*). Зокрема, термін «збирання» у цьому контексті не зводиться до фіксації інформації, а охоплює фізичне вилучення носіїв. Натомість «здобуття» стосується створення копії, що має особливу значущість у контексті забезпечення цілісності оригіналу. Утворення образу є формою здобуття, яка дозволяє відтворити стан носія з побітовою точністю. Відсутність таких розмежувань у КПК України створює нормативну прогалину, яку може бути усунуто через імплементацію техніко-правових норм.

По-друге, стандартизоване визначення цифрового доказу як бінарної інформації, що може мати доказове значення, дозволяє охопити як дані, так і метадані, що є істотними для процесуального аналізу. У межах кримінального

процесу це підтверджує, що джерелом доказу є не лише безпосередній файл, але й структурний контекст його існування в цифровому середовищі.

Третє, вкрай важливими є категорії геш-значення, функція верифікації, збіжність і відтворюваність. Ці терміни мають пряме значення для оцінки вірогідності та допустимості доказів. Наприклад, отримання однакових геш-значень за однакових або різних умов є критерієм незмінності цифрового об'єкта, що має підтверджуватися під час процесуального дослідження.

Окремого аналізу потребує термін DEFR і DES. З одного боку, ці категорії підтверджують потребу в чіткому фаховому розмежуванні ролей під час взаємодії з доказами електронної форми. З іншого боку, в кримінальному процесі України відсутня пряма регламентація подібних суб'єктів, а отже — виникає потреба в нормативному закріпленні (можливо, на рівні підзаконних НПА) їх функціональних повноважень, обов'язків і відповідальності. Аналогом DES у КПК України спеціаліст, якого залучено для технічної підтримки слідчих дій (ст. 71 КПК України), однак цього статусу недостатньо для виконання повного спектра завдань, які описані в стандарті. При цьому DEFR, за відсутності залученого спеціаліста, можуть виступати навіть слідчий чи прокурор, технічні знання яких, а особливо таких складних, викликають сумніви.

Наведений в ДСТУ ISO/IEC 27037:2017 термінологічний апарат стандарту створює передумови для імплементації окремих дефініцій або принаймні їх адаптацію через підзаконні НПА, відомчі інструкції чи СОП.

Розділ 4 ДСТУ ISO/IEC 27037:2017 визначає перелік аббревіатур, що відображають міждисциплінарну природу стандарту та його опору на широкий спектр понять, що охоплюють як технічну інфраструктуру, так і професійні ролі, пов'язані з обробленням доказів електронної форми.

З огляду на обмежений обсяг цього дисертаційного дослідження розділи 5-7 ДСТУ ISO/IEC 27037:2017 детально не аналізуються, однак варто відзначити окремі положення.

Розділ 5 ДСТУ ISO/IEC 27037:2017 вибудовує загальну методологічну рамку початкової роботи з доказами електронної форми. Відповідно до пункту 5.4 ДСТУ

ISO/IEC 27037:2017 процес обробки доказів електронної форми включає: ідентифікацію (identification), збирання (collection), здобуття (acquisition) та збереження (preservation).

Відповідно до п.п. 5.4.2 ДСТУ ISO/IEC 27037:2017 процес ідентифікації (identification) включає пошук, розпізнавання та документування потенційного доказу (включаючи пошук прихованих електронних носіїв інформації та пристроїв). Він включає також визначення пріоритетів збирання доказів електронної форми з огляду на їх несталість (тобто пріоритетом є документування оперативної пам'яті порівняно з енергонезалежними електронними носіями інформації, що не інтегровані до ІС – прим. авт.).

Підпункт 5.4.3 ДСТУ ISO/IEC 27037:2017 визначає процес збирання (collection) доказів електронної форми а пп. 5.4.4 – їх здобуття (acquisition). Збирання в такому разі описується як фізичне вилучення відшуканого технічного пристрою або електронного носія інформації. Буквально – його переміщення з первісного місця розташування до лабораторії або іншого контрольованого середовища для подальшого здобуття. Процес збирання також передбачає захист від втрати чи пошкодження й належне пакування. Здобуття (acquisition) описується як процес створення копії та документування використовуваних методів і застосованих дій. Приклад: створення копії повного жорсткого диска, його частини або вибраних файлів.

Збереження (preservation) визначено в пп. 5.4.5 ДСТУ ISO/IEC 27037:2017 й описується як захист від втручання та псування потенційного доказу та технічних пристроїв, що можуть містити докази досліджуваної нами категорії. Процес збереження (preservation) має бути розпочатим та підтримуватися протягом всього часу роботи з доказом, починаючи з його ідентифікації. Відповідний процес має засвідчити, що доказ не було модифіковано з моменту, коли його було зібрано (collection) або здобуто (acquisition), або ж логічно обґрунтувати та задокументувати всі дії, якщо невідворотні зміни все ж було внесено.

Розділ 6 ДСТУ ISO/IEC 27037:2017 визначає ключові компоненти ідентифікації, збирання, здобуття та збереження доказів електронної форми. Варто

окремо звернути увагу на Пункт 6.1 ДСТУ ISO/IEC 27037:2017 визначає хронологічне документування (ланцюгазбереження доказів, chain of custody) як базовий елемент забезпечення цілісності, достовірності та допустимості доказів електронної форми.

Отже, ДСТУ ISO/IEC 27037:2017 має надзвичайно важливе значення для вдосконалення практики роботи з доказами електронної форми під час кримінального провадження. У межах цього дослідження неможливо охопити весь ДСТУ ISO/IEC 27037:2017 з огляду на його великий обсяг та обмежені розміри нашої праці. На нашу думку, перспективним напрямком подальших наукових досліджень у цій сфері, запланованих автором на майбутнє, є підготовка науково-практичного коментаря до ДСТУ ISO/IEC 27037:2017, що стане основою для розробки СОП у сфері роботи з доказами електронної форми під час кримінального провадження.

4.4. Зарубіжний досвід роботи з доказами електронної форми в кримінальному процесі

Сучасна цифрова епоха суттєво змінила характер доказування у кримінальних справах. Докази електронної форми набувають все більшого значення у практиці правоохоронних органів і судів. Згідно з проведеним нами опитуванням суб'єктів кримінального провадження, в Україні у кримінальних провадженнях середній рівень «присутності» доказів електронної форми становить 53,4%, що ілюструє їх високу розповсюдженість та є відверто величезним значенням з огляду на системні недоліки правового регулювання в цій сфері [114, с. 78-79]. В США, Канаді та ЄС ця частка складає близько 80 %. Це зумовлено широким використанням цифрових технологій у повсякденному житті, як наслідок – сліди злочинів все частіше існують у формі електронних даних [435, с. 34].

ЄС приділяє значну увагу регулюванню доказів електронної форми. Головним досягненням у цьому напрямі є «пакет електронних доказів» (e-evidence package), ухвалений у 2023 році. Він складається з двох взаємопов'язаних актів: Регламент (ЄС) 2023/1543 про Європейські ордери на надання та збереження електронних доказів у кримінальних провадженнях та для виконання покарань, пов'язаних з позбавленням волі, після кримінальних проваджень [490, с. 1] та супутня Директива (ЄС) 2023/1544, що встановлює гармонізовані правила щодо визначення установ та призначення юридичних представників з метою збору електронних доказів у кримінальних провадженнях [378, с. 1]. Ці документи закладають нову європейську систему доказів електронної форми і застосовується з 18 серпня 2026 року. Встановлено, що Директива повинна бути перенесена до національного законодавства держав-членів ЄС до 18 лютого 2026 року. Передумовою регламенту була Директива 2014/41/ЄС про Європейський наказ про розслідування [380, с. 1]. Попри введення власного механізму, в ЄС паралельно ведеться робота над міжнародними угодами. По-перше, це Другий додатковий протокол до Конвенції про кіберзлочинність. По-друге, Єврокомісія у 2019 році отримала мандат на переговори зі США про угоду ЄС-США щодо доказів

електронної форми [424]. Чутливою сферою для ЄС є баланс між потребами правоохоронних органів та захистом персональних даних, що регулює Загальний регламент із захисту даних (GDPR) [489, с. 1]. Для узгодження колізій ЄС розробляє власні інструменти [378, с. 1] та веде переговори про міжнародні угоди (як із США) [424]. В ЄС проблема взаємного визнання доказів електронної форми між країнами-членами вирішується через механізми міжнародної правової допомоги та новітні інструменти як Європейський наказ про надання електронних доказів (European Production Order, ЕПОС) та Європейський наказ про збереження електронних доказів (Preservation Order, ЕПОС-PR), що застосовуватимуться з 18 серпня 2026 року. Отже, докази електронної форми стали невіддільною частиною сучасного кримінального процесу ЄС, але вимагають спеціальної уваги до процедур їх отримання, перевірки та використання [435, с. 36-37].

Правова система Великої Британії не кодифікує поняття доказу електронної форми (електронного доказу, цифрового доказу), окремо – цифрові дані підпадають під загальні правила доказування англійського права [474; 535]. Водночас Велика Британія має окреме законодавство щодо перехоплення комунікацій та отримання даних від провайдерів [426]. Британські суди накопичили практику щодо використання доказів електронної форми у різноманітних справах – від кіберзлочинів до традиційних злочинів, де ключовими доказами виступають записи з камер CCTV, SMS-повідомлення, дані геолокації телефонів тощо [525]. У галузі кіберзлочинності показовими є кейси, де британські суди зіштовхуються з доказами, зібраними за кордоном або наданими іноземними інтернет-компаніями. До 2020 року така співпраця йшла переважно шляхом договорів про взаємну правову допомогу (MLAT), але після укладення угоди між США та Британією за CLOUD Act (2019) [308] отримання від американських провайдерів доказів електронної форми значно прискорилося. Приміром, у розслідуванні терористичних злочинів британські слідчі можуть напряму (за погодженою процедурою) запитувати дані з американських соцмереж, замість довгого MLAT-процесу. Британські суди уже мають справи, де використано такі швидко отримані дані, і виробляється практика оцінки їх допустимості.

Велика Британія відома своєю Настановою АСРО щодо цифрових доказів. Вперше розроблена Асоціацією головних офіцерів поліції (АСРО) у 2007 році, ця Настанова (остання версія 5.0 вийшла 2012 р.) [302, с. 1] встановила чотири основні принципи роботи з доказами електронної форми включно з уже згаданим принципом про незмінність даних. Інші принципи АСРО вимагають, щоб усі дії з цифровим носієм виконували тільки кваліфіковані особи, щоб при кожному доступі до даних фіксувалися всі дії (аудит-трейл), а відповідальність за дотримання закону ніс старший офіцер, який контролює слідчу дію.

Крім того, у Британії діє Регулятор судової експертизи (Forensic Science Regulator), який видає обов'язкові кодекси практики для судово-експертних установ. У 2017 році Регулятор випустив окремий кодекс щодо цифрової криміналістики [359], де встановив вимоги до лабораторій, що проводять аналіз комп'ютерів, мобільних телефонів тощо (калібрування інструментів, валідація методик, компетентність персоналу) [435, с. 37-38].

В Кодексі кримінальної процедури Франції (Code de procédure pénale, CPP) [355, с. 1] прямого визначення понять «доказ електронної форми», «електронний доказ» або «цифровий доказ» немає, але законодавець передбачив низку спеціальних інструментів для отримання цифрових даних. Так, для боротьби зі злочинами, пов'язаними з ІТ, були введені положення про комп'ютерне стеження (ст. 706-102-1 CPP), що дозволяє слідчим органам здійснювати приховане перехоплення комп'ютерних даних (наприклад, встановлення шпигунського ПЗ) за судовим рішенням у справах про тяжкі злочини (положення про комп'ютерне стеження (ст. 706-102-1 CPP) застосовуються лише у тяжких кримінальних справах (тероризм, організована злочинність), і на підставі рішення судді). Інші статті (706-95-1 та 706-95-2 CPP) регулюють наказ про надання збережених даних – слідчий суддя може зобов'язати провайдерів надати наявні у них електронні листи, повідомлення тощо. Для перехоплення контенту в режимі реального часу (наприклад, читання нових електронних листів у міру їх надходження) застосовуються положення про прослуховування (ст. 100 та ін. CPP), за аналогією з телефонними прослуховуваннями. Таким чином, французьке законодавство

інтегрує цифрові канали зв'язку у вже наявні механізми слідства (обшуки, виїмки, прослуховування), водночас доповнюючи їх спеціальними нормами для кіберпростору.

У 2016 році Франція також оновила законодавство, надавши слідчим широкі повноваження у сфері цифрових розслідувань під час надзвичайного стану та антитерористичних операцій [314, с. 1].

Французькі суди традиційно визнають принцип свободи доказування у кримінальних справах – суд може враховувати будь-які докази, якщо вони здобуті законно і надійні [498]. Докази електронної форми в цьому контексті не є винятком. Наприклад, суди приймали як докази роздруківки електронних листів, SMS-повідомлень, дані GPS трекерів тощо [407, с. 1]. У цивільному процесі у Франції вже давно діє закон про електронні підписи, який прирівнює правильно підписаний e-Mail до паперового документа [445, с. 1]. Аналогічно, судова практика підтвердила, що SMS-повідомлення, отримані без шахрайства, можуть використовуватися як докази [354, с. 1].

Французькі правоохоронні органи активно використовують докази електронної форми в розслідуванні тероризму та організованої злочинності. Гучний міжнародний випадок – злам за допомогою французької жандармерії шифрованої мережі EncroChat у 2020 році, в результаті чого отримано мільйони зашифрованих повідомлень злочинців по всій Європі. Ці дані були використані як докази у сотнях кримінальних справ (в тому числі в Німеччині, Нідерландах, Франції). Французькі суди визнали законність отримання таких доказів, оскільки операція проводилась на території Франції з дозволу суду, і згодом дані передавалися в інші країни каналами правової допомоги [412, с. 1]. Цей випадок підкреслив важливість міжнародної співпраці та обміну доказами електронної форми.

У Франції, як і в інших країнах ЄС, діють рекомендації Інтерполу [416] щодо роботи з доказами електронної форми. Поліцейські та жандармерія керуються інструкціями щодо вилучення комп'ютерної техніки (як упакувати, як зберігати). Існує національний підрозділ C3N (Centrale Cyber de la Gendarmerie), що

спеціалізується на цифрових розслідуваннях і напрацьовує методичні рекомендації для слідчих [408, с. 1]. Франція також учасник Конвенції про кіберзлочинність, і відповідно впровадила у своє законодавство її положення [374, с. 1]. На рівні ЄС Франція впровадила Європейський наказ про розслідування (директива 2014/41/EU), що спрощує визнання і виконання запитів на отримання доказів між державами-членами [468, с. 1]. Таким чином, французька система стоїть на поєднанні національних норм і європейських механізмів, що дозволяють ефективно оперувати доказами електронної форми [435, с. 38-39].

У Німеччині не існує у законі окремого поняття цифрового доказу. Усі докази (включно з тими, що мають електронну форму) підкоряються принципу вільної оцінки доказів судом (*Grundsatz der freien Beweiswürdigung*) згідно з Кримінального процесуального кодексу Німеччини (*Strafprozessordnung, StPO*) [411, с. 1]. Однак законодавство розвивається в напрямку цифровізації прикладом чого є поява в *StPO* статей про онлайн-перехоплення і комп'ютерний пошук. У 2008 році Федеральний конституційний суд Німеччини у рішенні щодо онлайн-обшуку (справа про Північний Рейн-Вестфалія) постановив, що негласне проникнення держави в комп'ютер особи є дуже серйозним втручанням у приватність, і допустимим лише за наявності конкретної загрози найвищим благам (наприклад, життя людей, держбезпеці) і при дотриманні процедурного захисту (судовий ордер, контроль) [528, с. 1]. У відповідь на це рішення до *StPO* були внесені зміни: з'явився §100b, що дозволяє таємний дистанційний обшук інформаційних систем (*Quellen-TKÜ i Online-Durchsuchung*) за строго визначених обставин. Також §100a оновлено щодо перехоплення телекомунікацій, включно з інтернет-комунікаціями [467, с. 1]. Таким чином, зараз німецькі слідчі мають правову можливість отримувати докази електронної форми з комп'ютерів або через мережі, але під контролем суду і лише в тяжких справах (наприклад, тероризм).

У Німеччині питання допустимості доказів часто вирішується в контексті забезпечення конституційних прав. Наприклад, якщо доказ електронної форми, отримано із порушенням прав на приватність або без належного дозволу, захист може вимагати визнати його недопустимим на підставі доктрини

Verwertungsverbote [375, с. 1] (заборони використання доказів). Суд може виключити доказ, здобутий шляхом, що явно порушує закон (наприклад, якщо поліція зламала телефон без ордеру). Нерідко такі питання доходять до Федерального конституційного суду [488, с. 1]. Що стосується автентифікації доказів електронної форми німецька традиція менш формалізована, ніж англо-американська. Немає аналогів правил про самоавтентифікацію; натомість, якщо сторона заперечує справжність, суд призначає експертизу або досліджує доказ у судовому засіданні [450].

Німеччина, маючи федеративний устрій, не має єдиного національного керівництва на кшталт британського АСРО, але федеральна поліція (ВКА) та земельні кримінальні відомства (ЛКА) розробляють свої інструкції з цифрової криміналістики. Суттєву роль відіграють європейські стандарти (наприклад, Європейська мережа судової експертизи ENFSI має експертну групу з цифрових доказів, напрацьовано загальні керівні принципи) [319].

У Німеччині поліцейські органи системно нарощують спроможності з роботи з електронними доказами: у складі ВКА функціонують підрозділи IT-forensik та цифрової електроніки, які здійснюють вилучення, збереження, аналіз і відновлення даних з носіїв, а також розробляють методики й інструменти для слідства [432]. На рівні земель діє мережа криміналістичних IT-лабораторій [527, с. 1]. Для пришвидшення обробки великих масивів даних ЛКА підключаються до створюваної ВКА інтегрованої «Untersuchungs- und Auswertumgebung (IUA)»; проект і його впровадження фіксуються як на федеральному рівні (матеріали Бундестагу) [313], так і в повідомленнях земельних (напр., Бранденбург) [420]. Попри інвестиції, медіа та профспілки вказують на «вузькі місця»: за даними Welt am Sonntag із посиланням на поліцейські джерела та BDK, у складних провадженнях аналіз одного носія може тривати до 18 місяців; водночас поліція повідомляє про запуск нових лабораторій і розширення парку засобів обробки [418, с. 1]. ВКА та поліції земель також ведуть постійні набори спеціалістів «Cyber & Digital Forensics», що відображає структурне розширення кадрового потенціалу в IT-криміналістиці [431, с. 1]. Таким чином, Німеччина робить акцент на

інституційній спроможності опрацьовувати докази електронної форми (підготовка кадрів, технічне оснащення, методики), а правове регулювання імплементує поступово у відповідь на виклики, забезпечуючи при цьому відповідність Конституції [435, с. 39].

Сполучені Штати Америки не мають єдиного кодифікованого акта щодо доказів електронної форми проте низка законів і нормативних актів регулює різні аспекти роботи з цифровою інформацією в кримінальному процесі. Загальні вимоги до допустимості доказів – у тому числі тих, що мають електронну форму – встановлено Федеральними правилами доказів (Federal Rules of Evidence, FRE) [406, с. 1]. У 2017 році до них внесено поправки, що спростили використання доказів електронної форми (902(13) та 902(14)) [494].

Для отримання електронної інформації під час слідства у США діє ряд законів, які визначають порядок доступу правоохоронців до даних, що зберігаються у провайдерів зв'язку та інтернет-сервісів: Electronic Communications Privacy Act (ECPA) [300, с. 1] та його складова – Stored Communications Act (SCA) [301, с. 1], які встановлюють процедури отримання контенту електронних комунікацій, метаданих тощо на підставі судових ордерів, запитів, повісток залежно від типу інформації. У 2018 році Конгрес США ухвалив закон CLOUD Act (Clarifying Lawful Overseas Use of Data Act) [353; 514], що прямо дозволив американським правоохоронцям за наявності судового ордеру отримувати дані, які знаходяться на серверах за кордоном, а також спростив укладення міжнародних угод про доступ до доказів електронної форми [471]. Важливою для розвитку цифрового законодавства США стала справа *Microsoft Corp. v. United States*, продемонструвавши межі юрисдикції за відсутності чітких норм щодо екстериторіального доступу до даних [508]. Одним із провідних прецедентів є рішення Верховного Суду США у справі *Riley v. California* (2014) [509], де одноголосно встановлено, що поліція зазвичай зобов'язана отримати судовий ордер для обшуку вмісту мобільного телефону, вилученого при арешті особи. У справі *Lorraine v. Markel* (2007, окружний суд США; це рішення окружного суду (District of Maryland), яке стало широко цитованим, але не є прецедентом

Верховного суду США) було детально проаналізовано критерії допустимості різних видів доказів електронної форми (автентичність, недопустимість чуток, належність і цілісність) і наголошено, що принципи доказування однакові для електронної і традиційної інформації, хоча практичне їх застосування може відрізнятися через технічні нюанси [392; 433]. Також у США розроблено численні посібники для правоохоронців щодо роботи з цифровими доказами [516; 376; 480; 377]. Хоча ці документи не мають сили закону, вони слугують *de facto* стандартами й часто згадуються в суді при оцінці належності дій слідства з доказами електронної форми.

Однією з основних юридичних колізій, пов'язаних з CLOUD Act, є конфлікт з Загальним регламентом захисту даних (GDPR) ЄС. Згідно з GDPR передача персональних даних за межі ЄС можлива лише за наявності відповідних правових гарантій — наприклад, міжурядових угод або адекватних запобіжників [423]. З одного боку, американський CLOUD Act 2018 року, як вже згадувалося, вимагає від постачальників послуг, підсудних юрисдикції США, надавати дані на виконання американських ордерів чи запитів — незалежно від того, де фізично зберігаються ці дані. З іншого боку, європейський GDPR (Регламент (ЄС) 2016/679) встановлює суворі правила передачі персональних даних за межі ЄС: така передача може відбуватися або до країн з адекватним рівнем захисту, або на основі встановлених механізмів (стандартні контрактні положення, Privacy Shield — який було скасовано, зараз готується заміна), або відповідно до винятків, прямо передбачених (стаття 49) [489, с. 1]. Звичайний запит іноземної влади не входить до цих підстав, ба більше, як зазначено в ст. 48 GDPR, рішення суду чи адміністративного органу третьої країни, що вимагає передати дані, не визнається, якщо тільки між країнами нема міжнародної угоди. У 2019 році Європейська рада і Комісія опублікували спільну заяву, що переговори з США про взаємний доступ до доказів електронної форми є пріоритетними, і що без такої угоди конфлікти права неминучі [434, с. 1]. Європейська комісія загалом зайняла прагматичну позицію: CLOUD Act розглядається як реальність, з якою треба рахуватися, тому слід укласти двосторонню угоду, котра б визначила гарантії та процедури [519,

с. 1]. Європейська рада із захисту даних (EDPB) та Європейський наглядовий орган із захисту даних (EDPS) у липні 2019 року подали спільний юридичний аналіз впливу CLOUD Act. [384; 40-41].

Кримінально-процесуальний кодекс Латвії [439, с. 1] передбачає можливість фіксації доказів у електронному форматі та їх подальшого використання (ст. 127, 135, 136) [102, с. 91].

В Кримінально-процесуальному кодексі (далі – КПК) Литви закріплено норми щодо фіксації доказів у електронному форматі та їх використання під час судового розгляду. Пункт 4 ч. 1 ст. 96 КПК Литви до документів зараховує електронні носії інформації, а в ч. 2 ст. 290 КПК Литовської Республіки окремо акцентовано, що докази у формі аудіозаписів та відеозаписів, зроблені під час досудового розслідування під час судового розгляду можуть бути прослухані та переглянуті [317, с. 1].

Кримінально-процесуальний кодекс Естонії [438, с. 1] визначає широкий спектр процесуальних інструментів та процедур, що становлять електронний сегмент кримінального провадження, зокрема: електронна комунікація між суб'єктами кримінального провадження, електронні інструменти кримінального процесу, електронна форма доказів, електронна форма процесуальних документів, електронна форма реалізації слідчих дій та негласних слідчих дій, дистанційний формат реалізації процесуальних процедур, електронна фіксація кримінального провадження [103, с. 213]. До доказів у ч. 1 ст. 63 КПК Естонії [438, с. 1], окрім іншого, віднесено, відеозапис слідчої дії, судового засідання і оперативно-розшукового заходу, а також інший документ, фото, відеозапис або інший носій інформації. Відповідно до ч. 3 ст. 149 КПК Естонії, цифрова фотографія наводиться в протоколі процесуальної дії або в якості додатку до нього, і зберігається у вигляді комп'ютерного файлу в системі електронного справи «e-toimik» [103, с. 214].

Швейцарська модель регулювання роботи з доказом електронної форми виходить із технологічно нейтральних норм про обшук і тимчасове вилучення «записів» та «носіїв інформації» [496; 324; 517].

У контексті кримінального процесу Швеції правове регулювання застосування доказів електронної форми характеризується певною гнучкістю, хоча й водночас відзначається відсутністю спеціалізованих процедурних правил, які б прямо регламентували їх автентичність чи достовірність [486, с. 1]. Судова практика Швеції допускає використання цифрових комунікацій, збережених даних, інтернет-документів [391].

Правове регулювання доказу електронної форми у кримінальному процесі Фінляндії спирається на поєднання загальних правил доказування та спеціальних інструментів доступу до цифрових джерел. Оцінка допустимості, належності та достовірності здійснюється за загальними приписами [358, с. 1]. Відповідні норми інтегруються у провадження як доказ електронної форми з подальшою судовою перевіркою автентичності та цілісності [361, с. 1]. Також визначено стандарти збирання і документування матеріалів, включно з цифровими записами [473].

Нормативне регулювання доказів електронної форми в Данії інтегроване у Закон про відправлення правосуддя, насамперед у розділ про втручання в таємницю повідомлень та пов'язані слідчі дії [443; 352].

Кримінальний процесуальний кодекс Норвегії не містить спеціалізованої норми, що окремо регламентувала б докази електронної форми, однак передбачає загальні засади допустимості та належності доказів [515]. Спеціальною новелою є внесення в 2017 р. поправки до § 199 а Кодексу, що дозволяє правоохоронним органам вимагати від особи, котра має доступ до системи обробки даних, розблокувати її за допомогою біометричної автентифікації (зокрема, силою) з метою одержання даних [322].

Правове регулювання доказу електронної форми в Ісландії зосереджене у Кодексі кримінального провадження Ісландії (*Lög um meðferð sakamála* № 88/2008). Положення про накладення арешту на речі визначає, що арешт може бути накладено як на матеріальні носії, так і на інформаційні потоки, зокрема на листи, телеграми, електронні листи тощо [447].

Правове регулювання доказів електронної форми в кримінальному процесі Нідерландів будується на загальних правилах допустимості та оцінки доказів.

Зокрема, норми про обшук з метою фіксації даних, що зберігаються на носіях інформації, і копіювання таких даних, надають слідчим суддям і органам досудового розслідування інструменти для вилучення цифрових масивів без обов'язкової матеріальної конфіскації носія [531; 436]. Також Нідерланди імплементують європейський режим e-Evidence для обміну доказами електронної форми в кримінальних провадженнях. При цьому Уряд Нідерландів відзначає, що у більш ніж половині кримінальних справ цифрові докази є вирішальними [463, с. 1]

Кодекс кримінального процесу Люксембургу встановлює підстави та порядок проведення обшуку, виїмки і примусових слідчих дій, що охоплюють отримання та фіксацію комп'ютерних даних, а також відстеження телекомунікацій; відповідні повноваження деталізовано, зокрема, у статтях 33, 47, 65 і 67-1, включно із можливістю «захоплення комп'ютерних даних» [356; 448]. Спеціальне регулювання у сфері електронних комунікацій та суміжних сервісів забезпечує зберігання й надання даних провайдерами у межах кримінального провадження [449].

В кримінальному процесі Італії після імплементації Конвенції про кіберзлочинність з'явилися прямі посилання на цифрові носії; питання автентичності й цілісності окремо не врегульовані та вирішуються поєднанням кримінальних процесуальних норм і судової практики [441].

Кримінально-процесуальний кодекс Сингапуру надає органам розслідування повноваження одержувати доступ до комп'ютерних систем, включно з віддаленим доступом, що забезпечує процесуальну придатність цифрових джерел для формування доказу електронної форми [371; 397; 398].

Кримінальний кодекс Канади встановлює спеціальні інструменти доступу до даних, включно з приписами про збереження та надання комп'ютерних даних, що структурує процесуальні підстави для одержання і фіксації доказів електронної форми [369]. Судова практика підкреслює баланс між ефективністю розслідування та захистом приватності у цифровому середовищі, що прямо впливає на оцінку допустимості і способів збирання доказів електронної форми [482; 483].

У правовій системі Китаю докази електронної форми фактично інтегровано через електронні дані [372]. Наукові дослідження акцентують на труднощах належного вилучення, збереження, автентифікації та оцінки доказу електронної форми: наприклад, ряд авторів вказують на відсутність спеціального закону про електронний доказ і недостатню деталізацію кримінальних процедурних норм [533; 381].

Південна Корея сформувала комплексну нормативну основу цифровізації кримінального судочинства. Зокрема, визначено порядок подання, зберігання та використання електронних документів і доказів електронної форми в судових процесах [306]. Додатково діє закон, що забезпечує технічну інфраструктуру електронного документообігу [305]. Кримінально-процесуальний кодекс Південної Кореї визнає право сторін на ознайомлення і копіювання матеріалів у електронній формі, що підтверджує процесуальну легітимність використання цифрових носіїв як джерел доказів [370]. У межах судової системи функціонує електронна платформа «e-Trials», яка дозволяє подавати й переглядати матеріали справи, включно з доказами електронної форми, без фізичної присутності [393]. Допустимість доказів електронної форми залежить і від дотримання гарантій законності під час їх одержання [479]. Також законодавство про захист персональної інформації зобов'язує забезпечувати конфіденційність та цілісність персональних даних при їх використанні в кримінальному процесі [472]. Система електронного правосуддя передбачає суворе дотримання стандартів ідентифікації цифрових джерел, перевірки цілісності та можливості незалежного аудиту способів копіювання [540].

Правове регулювання доказів електронної форми у кримінальному процесі Японії ґрунтується на поєднанні загальних норм кримінального процесу та спеціального законодавства про електронні комунікації [303] й електронні підписи [304]. Кодекс кримінального процесу Японії встановлює процесуальні підстави й межі для обшуку, виїмки та огляду носіїв інформації, що дозволяє вилучення та дослідження електронних даних як різновидів речових доказів, із дотриманням судового контролю та вимог до постановлення і виконання судових рішень [357],

перехоплення комунікацій [368]. Це створює нормативну основу для інкорпорації цифрового елементу у доказову базу та визначає процесуальні гарантії їх допустимості, що також підтримується доктринальними положеннями [461].

В Гонконзі спостерігається високий рівень формалізації регулювання питання доказів електронної форми, зокрема щодо допустимості доказів електронної форми (computer-generated document) в кримінальному провадженні [536].

В Тайвані докази електронної форми фактично використовується, але нормативні визначення та спеціалізовані положення в кримінальному процесуальному законодавстві не визначені [444].

У Південній Африці є законодавча база для прийнятності доказів у формі електронних повідомлень [385], питання доказу електронної форми в кримінальному процесі потребують активнішої нормативної та практичної конкретизації [530].

В Законі про докази Малайзії розділи прямо регулюється прийнятність документів, створених комп'ютером («computer-generated documents») як доказів у кримінальних провадженнях [399], визначаються критерії їх оцінки [484].

В Об'єднаних Арабських Еміратах Закон про електронні транзакції та довірчі послуги встановлює, що прийнятність електронного документа, електронного підпису, електронної печатки чи електронних транзакцій «у будь-якому судовому провадженні» не може бути відхилена лише через електронну форму [404; 326]. У Законі про докази у цивільних і комерційних справах закріплено окрему главу про електронний доказ та його визначення й складники [402]. У кримінальному процесі суди застосовують ці загальні норми про доказ електронної форми разом із процесуальними приписами Кримінального процесуального закону щодо фіксації та оцінки доказів [403; 405].

У Саудівській Аравії Закон про докази прямо визнає доказ електронної форми, надаючи цифровим документам, записам і підписам доказову силу, еквівалентну письмовим [477, с. 1]. У кримінальному провадженні використання таких доказів здійснюється за загальними приписами Кримінального

процесуального закону щодо збирання, дослідження та оцінки доказів [442] і затверджені процесуальні керівництва Міністерства юстиції щодо «цифрового доказу» [476, с. 1].

У Кувейті Закон «Про протидію злочинам у сфері інформаційних технологій» містить матеріально-процесуальні механізми, орієнтовані на дані, інформаційні системи та їх використання як джерела доказу електронної форми у кримінальних справах [539].

У Катарі Закон «Про запобігання кіберзлочинності» упроваджує процесуальні інструменти, пов'язані з електронними системами та даними, що використовуються як джерело доказу електронної форми [478, с. 1]. Застосування таких доказів відбувається в межах загальних норм Кримінального процесуального кодексу Катару [487, с. 1].

В Кримінально-процесуальному кодексі Вірменії [538, с. 1] передбачено можливість фіксації доказів електронної форми та їх використання під час судового розгляду. Відповідно до ч. 2 ст. 121 КПК Вірменії, як докази можуть бути використані протоколи слідчих дій, зокрема: моніторинг листування, пошти, телеграфу та інших комунікацій (п. 8); прослуховування телефонних розмов (п. 9). Стаття 122 КПК Вірменії в ч. 1 визначає документом будь-який запис на паперовому, магнітному, електронному або іншому носії, що виконаний у словесній, цифровій, графічній або іншій знаковій формі, яким можуть бути засвідчені дані, що мають значення для кримінальної справи. Висновок експерта включає фотографії, що ілюструють висновки експерта (ч. 3 ст. 250 КПК Вірменії). В ч. 2 ст. 29 КПК Вірменії визначено вимоги до застосування технічних засобів, зокрема відеозапису, під час проведення слідчих дій. Такою ч. 2 ст. 29 КПК Вірменії вказує, що матеріали відеозапису не підлягають редагуванню чи зміні іншим чином [101, с. 206].

В Кримінально-процесуальному кодексі Грузії передбачено можливість використання під час судового розгляду аудіо- або відеозаписів показань свідків, отриманих під час досудового розслідування (ст. 243). Згідно з ч. 23 ст. 3 КПК Грузії документом (як доказом) вважається будь-яке джерело, в якому інформація

відображена в словесно-знаковій формі або (і) у вигляді фото-, відео-, звуко- або іншого запису, або із застосуванням інших технічних засобів. Також до висновку експерта повинні додаватися фотознімки, схеми та інші матеріали, які підтверджують висновок експерта (ч. 3 ст. 146 КПК Грузії) [97, с. 162].

В Кримінально-процесуальному кодексі Молдови [360, с. 1] передбачено можливість фіксації доказів у електронному форматі та їх використання під час судового розгляду. Допускається можливість відтворення аудіозаписів та відеозаписів таких показань підсудного (ч. 1 ст. 368 КПК Молдови), свідка (ч. 1 ст. 371 КПК Молдови) наданих ним під час досудового розслідування [98, с. 133-134]. Відповідно до ст. 157 КПК Молдови, документами як матеріальними засобами доказування виступають документи в будь-якій формі: аудіо, відео, електронній та ін.), надані офіційними фізичними або юридичними особами, якщо в них викладені або засвідчені обставини, що мають значення для справи. Згідно з ч. 3 ст. 88 КПК Молдови, експерт зобов'язаний у своєму висновку відокремити ті висновки, що отримані з використанням комп'ютерних програм [98, с. 133-134].

В Кримінально-процесуальному кодексі Азербайджану [315, с. 1] передбачено використання доказів, що зафіксовано в електронному форматі. Допускається оголошення показань обвинуваченого (ч. 1 ст. 327 КПК Азербайджану), свідка (ч. 1 ст. 329 КПК Азербайджану), наданих під час досудового провадження, в раніше проведеному або поточному судовому засіданні під час триваючого судового розгляду і відтворення аудіозапису, відео - або кіноплівки цих показань. Також, відповідно до ч. 1 ст. 135 КПК Азербайджану, документами визнаються паперові, електронні або інші носії, що відображають в собі у формі букв, цифр, графічних та інших знаків відомості, що можуть мати значення для кримінального переслідування [99, с. 118].

В Кримінально-процесуальному кодексі Туркменістану [518, с. 1] передбачено електронну форму фіксації доказів. Згідно з ч. 10 ст. 134 КПК Туркменістану, для фіксації доказів, поряд зі складанням протоколів, можуть застосовуватися звукозапис, відеозапис та фотозйомка. Звукозаписи, відеозаписи, фотографії, інші відображення ходу та результатів слідчої або судової дії

додаються до протоколу (ч. 11 ст. 134 КПК Туркменістану). У окремих випадках допускається відтворення долучених до протоколу допиту звукозаписів та відеозаписів показань підсудного, наданих у справі під час дізнання або попереднього слідства. Відповідно до п. 2 ч. 3 ст. 131 КПК Туркменістану, до документів відносяться матеріали, що містять комп'ютерну інформацію, фотографії, звукозаписи та відеозаписи [100, с. 92-93].

Отже, проведений порівняльно-правовий аналіз іноземного досвіду роботи з доказами електронної форми в кримінальному процесі дає підстави констатувати, що докази електронної форми перестали бути допоміжним елементом доказування і перетворилися на один із його системоутворювальних компонентів. Також доцільно окреслити тенденції правового регулювання іноземних держав щодо досліджуваного предмету, серед яких: інституціоналізація правового режиму доказів електронної форми у межах кримінального процесуального законодавства; утвердження технологічно нейтрального підходу до їх оцінки та допустимості (відсутність вимог визначених технічних засобів чи форматів); посилення вимог до автентичності, цілісності й простежуваності; запровадження спеціальних процесуальних механізмів для їх збирання, збереження та перевірки; уніфікація національних підходів із міжнародними стандартами.

Водночас, невід'ємною складовою іноземного досвіду роботи з доказами електронної форми в кримінальному процесі є використання електронних інформаційних систем для міжнародного обміну доказами під час кримінального провадження.

Міжнародні договори, зокрема і Конвенції про кіберзлочинність та Другий додатковий протокол до неї, закріплюють основи співпраці у цій сфері. КПК України в розділі IX регламентує порядок надання міжнародної правової допомоги, Однак відповідні норми КПК України не враховують у повному обсязі специфіку доказів електронної форми і не передбачають спеціальних процедур обміну ними за допомогою електронних інформаційних систем.

Міжнародне співробітництво правоохоронних органів є критично важливим елементом у боротьбі з транснаціональною злочинністю. Дослідники P. Thakkar, D.

Patel, I. Hirpara, J. Jagani, S. Patel, M. Shah та A. Kshirsagar (2023) [512] наголошують, що взаємодія між правоохоронними органами різних країн, координація спільних операцій та обмін інформацією необхідні для успішної протидії глобальним загрозам. С. М. Miller (2023) [457] підкреслює гостру потребу у зміцненні правоохоронних органів, що вимагає значних інвестицій їх у навчання та обладнання, де цифрові технології відіграють провідну роль у сучасних розслідуваннях, надаючи правоохоронним органам інструменти для ефективного збору, обробки та аналізу доказів. За словами J. Nosal (2023) [465], електронні системи значно прискорюють процес розслідування та зменшують ймовірність помилок або втрати важливих даних. G. Gupta та A. Husain (2023) [417] досліджують роль електронних систем у покращанні комунікації між правоохоронними органами в різних країнах, наголошуючи на важливості процесів розслідування. R. M. El-Kady (2023) [389] висвітлює досвід європейських країн у впровадженні систем електронного обміну доказами, відзначаючи їхній внесок у підвищення ефективності правоохоронної діяльності. M. Lukic-Radovic та M. Manojlovic-Nedeljkovic (2023) [452] підкреслюють важливість розширення застосування цифрових технологій для підвищення ефективності роботи правоохоронних органів а також потенціал розширення можливостей для залучення громадськості до моніторингу та контролю за дотриманням закону під час кримінальних розслідувань є недостатньо дослідженим питанням. R. Murachov (2023) [460] вивчає вплив платформ для обміну доказами електронної форми на покращення координації між різними юрисдикціями. На думку низки вчених [466], важливим аспектом є вдосконалення навичок роботи правоохоронців з електронними системами за допомогою регулярних тренінгів та освітніх програм. R. Stoykova та K. Franke (2023) [506] звертають увагу на роль нових технологій у забезпеченні прозорості та підзвітності процесів розслідування. M. Rojszczak (2020) [493] розглядає виклики, пов'язані з кібербезпекою та захистом даних при використанні електронних систем. Чимало робіт присвячено вивченню впливу цифрових технологій на захист конфіденційної інформації та кібербезпеку при обміні доказами [348], а також недолікам впровадження електронних систем в

контексті конфіденційності даних та забезпечення належного правового регулювання [499]. Науковці [456] наголошують на важливості міжнародного співробітництва та гармонізації правових стандартів для успішної інтеграції цифрових технологій у процес розслідування, а також необхідності розроблення та впровадження міжнародних стандартів для забезпечення ефективного обміну інформацією між країнами [351; 470, с. 4811–4812].

Спеціалізовані системи відіграють життєво важливу роль в обміні даними для формування доказової бази в кримінальних розслідуваннях. Однією з таких систем є електронні бази даних, що дозволяють правоохоронним органам зберігати, обробляти та обмінюватися великими обсягами інформації в цифровому форматі. Система ECRIS (European Criminal Records Information System) забезпечує швидкий обмін інформацією про судимості між країнами ЄС. Вона дозволяє здійснювати автоматизований запит та пошук інформації про судимості громадян, значно скорочуючи час обробки даних та підвищуючи точність інформації. Технічні особливості включають стандарти шифрування даних, багаторівневі системи доступу та автоматизовані механізми оновлення інформації, що забезпечують високу безпеку та конфіденційність [470, с. 4814].

Сучасний механізм міжнародного співробітництва у сфері кримінального провадження базується не лише на традиційних інститутах взаємної правової допомоги, а й значно посилюється завдяки впровадженню цифрових платформ і спеціалізованих систем. e-Evidence Digital Exchange – система, призначена для полегшення обміну доказами електронної форми між країнами ЄС. e-Evidence Digital Exchange підвищує швидкість та ефективність обміну доказами; знижує ризики безпеки даних. Вона передбачає створення безпечної децентралізованої системи між компетентними органами держав-членів, що дозволяє їм швидко та оперативно спілкуватися щодо електронного обміну в контексті Європейського ордера на розслідування та різних інструментів взаємної правової допомоги (Mutual Legal Assistance instruments, MLA) у сфері кримінального права [430, с. 1].

Secure Information Exchange Network Application (SIENA) – система, що експлуатується Європолем, призначена для безпечного обміну інформацією між

правоохоронними органами ЄС та іншими міжнародними партнерами. SIENA забезпечує високий рівень безпеки передачі інформації та підтримує широкий спектр типів доказів та інформації. SIENA також стала каналом обміну інформацією за замовчуванням для спеціалізованих правоохоронних підрозділів та різних ініціатив, таких як відділи повернення активів (ARO), центри співробітництва поліції та митниці (PCCC), підрозділи інформації про пасажирів (PIU), підрозділи фінансової розвідки (FIU), групи активного пошуку втікачів (ENFAST), спеціальні тактичні підрозділи (ATLAS), підрозділи Спільної цільової групи з боротьби з кіберзлочинністю (Joint Cybercrime Action Taskforce, J-CAT), ініціативи Nordic LOs initiative та Lake of Constance [497, с. 1].

Schengen Information System (SIS) – інформаційна система, яка підтримує обмін інформацією про правопорушників та розшукуваних осіб між країнами Шенгенської зони. SIS покращує координацію правоохоронних органів у боротьбі з транснаціональною злочинністю та забезпечує оперативний доступ до критично важливої інформації. SIS є найпоширенішою та найбільшою системою обміну інформацією для забезпечення безпеки та управління кордонами в Європі. Вона містить понад 90 мільйонів наборів даних. Оповіщення, внесені до SIS однією країною, стає доступним у режимі реального часу в усіх інших країнах, які використовують SIS, завдяки чому компетентні органи по всьому ЄС можуть знайти це оповіщення [524, с. 1].

INTERPOL's I-24/7 System (I-24/7) — це безпечна глобальна комунікаційна мережа, яка дозволяє 195 країнам-членам обмінюватися кримінальними даними та координувати свої дії в режимі реального часу. Вона забезпечує ефективну міжнародну співпрацю правоохоронних органів, допомагаючи боротися з транснаціональною злочинністю. I-24/7 посилює глобальну співпрацю між правоохоронними органами; забезпечує швидкий обмін важливою інформацією. Інтерпол використовує систему I-24/7 для швидкого обміну інформацією про злочини, підозрюваних і викрадені предмети. Вона працює цілодобово, дозволяючи правоохоронним органам різних країн обмінюватися інформацією в режимі реального часу [425, с. 1].

Використання електронних систем для міжнародного обміну доказами значно підвищує ефективність кримінальних розслідувань. Це збігається з висновками G. Rusman, E. D'orio, E. Popova та P. Kipouras (2023) [495], які підкреслюють важливість цифрових технологій для захисту конфіденційної інформації та кібербезпеки. Дослідження O. Dulskyi, T. Leliuk, V. Luhovyi, V. Melnyk та I. Morgun (2023) [382] підтверджує наші висновки про зниження ризику втрати або викривлення даних завдяки автоматизованим системам управління доказами. У роботі D. Sulisdyantoro та M. I. Marzuki (2023) [507] йдеться про важливість навчання правоохоронців для ефективного використання електронних систем.

Наведені у згаданих і багатьох інших наукових джерелах положення свідчать, що використання електронних систем у сфері міжнародного обміну доказами сприяє не лише зростанню ефективності кримінальних розслідувань, а й формуванню нових підходів до забезпечення безпеки та правової узгодженості у транснаціональному вимірі. Насамперед постає проблема кібербезпеки та конфіденційності даних. Електронні платформи обміну доказами передбачають передачу великих масивів інформації, у тому числі персональних даних, матеріалів слідчих дій та результатів технічних досліджень. Уразливість таких систем до кіберзагроз створює ризик несанкціонованого доступу, викривлення чи знищення доказів, що ставить під сумнів їхню автентичність та подальшу допустимість у судовому процесі. Другим викликом є відсутність уніфікації правових стандартів. Попри існування Конвенції про кіберзлочинність та Другого додаткового протоколу до неї, які встановлюють рамкові зобов'язання держав, національні правові системи зберігають значні відмінності у процедурах збирання, зберігання й передачі таких доказів. Колізії між юрисдикціями становлять ще одну суттєву проблему. Вони можуть виникати як у зв'язку з конфліктом національних норм про захист даних, так і внаслідок різних підходів до визначення меж міжнародної правової допомоги. Перспективи України у сфері міжнародного обміну доказами електронної форми визначаються передусім потребою створення комплексної та надійної системи їх захисту. Другим стратегічним напрямом є розроблення й

уніфікація стандартних протоколів та процедур для гармонізації правових аспектів обміну доказами електронної форми між різними юрисдикціями. Брак єдиних правил спричиняє правові колізії та ускладнює оцінку доказів судами, що знижує ефективність міжнародної співпраці. Гармонізація процесуальних норм на основі положень Конвенції про кіберзлочинність та Другого додаткового протоколу до неї має стати підґрунтям для вдосконалення національного кримінального процесуального законодавства, зокрема шляхом внесення змін до КПК України, які б прямо регулювали використання доказів електронної форми отриманих за допомогою міжнародних платформ. Третім пріоритетом є впровадження сучасних систем управління доказами, що забезпечують автоматизовану фіксацію, відстеження та аналіз усіх процесуальних дій із доказами. Такі системи дозволяють створювати детальний цифровий ланцюг збереження доказів (chain of custody), який фіксує кожний етап роботи з доказом, що унеможливорює сумніви щодо його достовірності. Автоматизація процесів не лише підвищує прозорість та підзвітність розслідувань, а й оптимізує міжнародний обмін інформацією, створюючи умови для ефективної інтеграції України до електронних систем ЄС та Інтерполу. Реалізація цих трьох ключових напрямів має бути підкріплена відповідними підзаконними актами, які визначатимуть технічні вимоги до систем захисту даних, регламентуватимуть порядок використання міжнародних платформ і забезпечуватимуть єдиний процесуальний підхід до доказів електронної форми. Важливим додатковим чинником залишається підготовка кадрів — без належної професійної компетентності слідчих, прокурорів і суддів навіть найдосконаліші системи не зможуть реалізувати свій потенціал [470, с. 4811–4812].

Отже, для кримінального процесу України пріоритетом є створення багаторівневої правової та технічної інфраструктури, що спиратиметься на три фундаментальні засади: надійний захист даних, уніфікацію правових процедур та запровадження сучасних систем управління доказами. Саме така модель дозволить гарантувати безпечний і стандартизований обмін доказами, посилить міжнародну співпрацю та зміцнить позиції України як активного учасника глобальної системи кримінальної юстиції.

РОЗДІЛ 5. ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ РОБОТИ З ДОКАЗАМИ ЕЛЕКТРОННОЇ ФОРМИ У КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ

5.1. Організаційні аспекти вдосконалення роботи з доказами електронної форми у кримінальному процесі України

Підсумовуючи результати дослідження, здійсненого у попередніх розділах, чи не найважливішим напрямом удосконалення роботи з доказами електронної форми в кримінальному процесі України можна вказати організаційну готовність суб'єктів кримінального провадження до роботи з доказами електронної форми, що передбачає дослідження відповідних аспектів.

Уніфікація підходів до підготовки юридичних та правоохоронних кадрів на рівні вищих навчальних закладів юридичного та правоохоронного профілів потребує навчання сучасним цифровим компетентностям. Формування сучасних практичних компетентностей у випускників правничих навчальних закладів України є важливою передумовою підготовки кваліфікованих кадрів, здатних забезпечити ефективну роботу з доказами досліджуваної категорії.

На нашу думку, формування прикладних знань і практичних навичок у випускників правничих шкіл України можливо забезпечити шляхом: широкого впровадження у юридичній освіті методу Case study (кейс-метод, або метод кейс-стаді) – інтерактивного методу навчання, що базується на обговоренні певного тексту, в якому відображається реальна неоднозначна ситуація в будь-якому виді людської діяльності. Case study сприяє розвитку вміння розв'язувати проблеми з урахуванням конкретних умов і за наявності фактичної інформації [265]; залучення до викладання прикладних та процесуально-правових юридичних дисциплін правників-практиків. Це допоможе студентам у засвоєнні не лише теоретичних знань, а й «живого» практичного досвіду, налагодженні професійних контактів; застосування під час викладання юридичних дисциплін сучасних педагогічних технологій: професійно-ділові ігрові технології; тренінгові засоби; інформаційно-

комп'ютерні технології [20, с. 28]; посилення ролі юридичних клінік у навчальному процесі. На нашу думку, для системного формування у студентів необхідних практичних компетентностей необхідне: впровадження нових та розширення діяльності існуючих юридичних клінік, залучення менторів з-поміж практичних працівників, відображення участі студентів у діяльності юридичної клініки в навчальному плані, що передбачає залучення до їх роботи кожного студента [124, с. 209-210].

Відповідність змісту юридичної освіти сучасним вимогам ринку праці та глобальним тенденціям розвитку професійної діяльності правників можна забезпечити шляхом запровадження навчальних дисциплін з вивчення електронного сегмента юридичної діяльності, основ кібербезпеки, роботи з базовими й галузевими (правничими) електронними інформаційними системами та базами даних. Зазначене актуалізує розроблення та системне впровадження навчальних дисциплін, пов'язаних з електронною складовою кримінального провадження. Важливою метою пропонованих курсів має бути введення студента в реальні життєві ситуації, прерогатива прикладного блоку навчальної дисципліни над теоретичним, невідкладна практична апробація отриманих знань та синхронне введення в суміжні дисципліни практичних блоків, що передбачають застосування отриманих навичок роботи з електронними інформаційними системами [124, с. 210].

Чинним КПК України передбачено функціонування численних електронних інформаційних систем. Під час кримінального провадження його суб'єктами застосовується з десятків відомих електронних інформаційних систем, що містять актуальну інформацію про кримінальне провадження та потенційно корисні практикам (та й студентам для формування відповідних практичних навичок). З огляду на це необхідно розробити і впровадити дисципліну «Електронні інформаційні системи органів кримінальної юстиції», синхронізувавши з курсом кримінального процесуального права. Ця окрема дисципліна необхідна зокрема через значний обсяг навчального матеріалу. А ось до навчальних дисциплін з

кримінального процесу України доцільно включити питання роботи з доказами електронної форми.

Отже, перспективними шляхами вдосконалення юридичної освіти щодо формування прикладних знань та практичних навичок у випускників правничих шкіл України, забезпечення змісту юридичної освіти вимогам ринку праці та глобальним тенденціям розвитку професійної діяльності правників є: широке впровадження у юридичній освіті методу Case study; залучення до викладання прикладних та процесуально-правових юридичних дисциплін практичних працівників відповідної правничої професії; застосування під час викладання юридичних дисциплін сучасних педагогічних технологій; посилення ролі юридичних клінік в навчальному процесі; запровадження навчальних дисциплін з вивчення електронного сегмента юридичної діяльності, основ кібербезпеки, роботи з базовими й галузевими (правничими) електронними інформаційними системами та базами даних [124, с. 211], роботи з доказами електронної форми під час кримінального провадження.

Чудовим прикладом прагматичного підходу до підготовки фахівців для системи кримінальної юстиції є Інститут СБУ Національного юридичного університету імені Ярослава Мудрого. Тут викладаються класичні, прикладні правничі та спеціальні навчальні дисципліни, далі курсанти проходять спеціальну підготовку за такими напрямками: досудове розслідування в органах СБУ; основи державної безпеки, контррозвідувальної та оперативно-розшукової діяльності; правове забезпечення оперативно-службової діяльності; інформаційна безпека та кібербезпека; тактико-спеціальна й оперативно-тактична підготовка; тактична медицина; керування БПЛА та квадрокоптерами; OSINT (розвідка на основі відкритих джерел); інші. Зауважимо, що до навчальних програм з кримінального процесу України [128; 291] включено і питання доказів електронної форми.

Розвиток ІТ та стрімке зростання кількості доказів електронної форми в кримінальних провадженнях, зумовлюють необхідність докорінної трансформації підходів до роботи. Загальноправова підготовка слідчих і прокурорів виявляється недостатньою для належної організації досудового розслідування та

процесуального керівництва з огляду на високий рівень технічної складності цифрового сегменту. Саме тому запровадження профільної спеціалізації слідчих та прокурорів у сфері кіберзлочинів слід розглядати як стратегічно важливий напрям вдосконалення діяльності органів досудового розслідування. Спеціалізований слідчий повинен мати не лише ґрунтовні правові знання, а й володіти комплексом компетенцій у галузі ІТ, комп'ютерної інженерії та кібербезпеки. Це забезпечить належну фіксацію, вилучення, збереження та дослідження доказів електронної форми а також підвищить ефективність співпраці з експертами та спеціалістами. Цю позицію поділяють і інші дослідники, приміром, Б. Б. Теплицький (2021) зазначає, що оскільки на етапі досудового розслідування обов'язок щодо оцінки зібраних доказів, у тому числі висновків судових експертів, та вирішення питання їх достатності для завершення розслідування покладається насамперед на слідчих та детективів, то для розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, враховуючи існуючу їх специфіку, має бути запроваджено відповідну спеціалізацію слідчих Національної поліції України, а також у вимогах до цих посад, окрім юридичної, слід передбачити необхідність професійно-технічної або вищої технічної освіти принаймні початкового рівня (короткого циклу) за відповідним напрямом [267].

Не менш важливим є питання спеціалізації прокурорів. Процесуальне керівництво у кримінальних провадженнях, пов'язаних із кіберзлочинами, потребує здатності прокурора не лише оцінити доказову базу з правової точки зору, а й критично осмислити її технічну специфіку. З огляду на зростання частки та ролі доказів електронної форми у структурі доказового масиву, прокурор повинен бути підготовлений до перевірки їх допустимості, достовірності, що вимагає встановлення їх цілісності та автентичності. Наявність прокурорів, що спеціалізуються на зазначених питаннях, сприятиме формуванню єдиної практики оцінки таких доказів та підвищить якість процесуального керівництва та підтримання публічного обвинувачення. Водночас слід підкреслити, що

запровадження спеціалізації прокурорів потребує всебічного обговорення з огляду на організаційну складність і значні кадрові ресурси.

Щодо судової системи, то ідея створення спеціалізованого кіберсуду видається передчасною. Попри стрімке зростання кількості кримінальних проваджень щодо кіберзлочинів, на сучасному етапі судова влада має достатні механізми для їх розгляду в межах загальної юрисдикції. Судді володіють необхідними процесуальними інструментами для оцінки доказів, у тому числі тих, що мають електронну форму, та можуть залучати фахівців у разі потреби. Запровадження ж окремого кіберсуду або спеціальної суддівської кваліфікації на даному етапі було б надмірним і могло б призвести до невиправданої фрагментації судової системи. Водночас не можна виключати, що у перспективі, за умов подальшого ускладнення характеру злочинності у сфері ІТ та суттєвого збільшення навантаження на судову систему, питання спеціалізованої юрисдикції може бути актуалізоване. Таким чином, оптимальною моделлю на сучасному етапі розвитку є запровадження профільної спеціалізації слідчих та поступове формування спеціалізації прокурорів із подальшою оцінкою ефективності таких заходів.

Створення криміналістичних ІТ-лабораторій у структурі правоохоронних органів, що структурно відокремлені від органів досудового розслідування та організаційно їм не підпорядковані є ще одним перспективним напрямом ефективної організації роботи з доказами електронної форми під час кримінального провадження. Прикладом такої інституційної моделі є криміналістична ІТ-лабораторія НАБУ, яка успішно функціонує у системі антикорупційної інфраструктури. Діяльність цього підрозділу довела доцільність поєднання технічної автономії та процесуальної взаємодії з органами досудового розслідування. Організаційна відокремленість криміналістичних ІТ-лабораторій повинна передбачати пряме підпорядкування керівництву відповідного правоохоронного органу без можливості тиску чи контролю з боку слідчих підрозділів або регіональних керівників. Подібним чином функціонують підрозділи кіберполіції та управління стратегічних розслідувань в структурі Національної поліції України (однак в аспектів оперативних працівників), що

забезпечує їх автономність та незалежність. Пропонована нами структурно відокремлена модель її побудови дозволяє зберігати об'єктивність та неупередженість у дослідженні доказів електронної форми оскільки їх працівники не підпорядковуються безпосередньо слідчому або прокурору, а діють у межах власної організаційної структури, виконуючи процесуальні завдання у межах вимог законодавства та на підставі процесуальних доручень. Саме структурна незалежність дозволяє мінімізувати ризик маніпуляцій та забезпечує високий рівень довіри до результатів проведених досліджень. Функціональне призначення таких лабораторій полягає у реалізації її фахівцями функцій DEFR на етапі пошуку та фіксації доказів електронної форми а також повноцінної їх роботи на всіх етапах кримінального провадження. Таким чином, створення криміналістичних ІТ-лабораторій у структурі правоохоронних органів України з відокремленим статусом є обґрунтованим кроком, що довів свою ефективність.

Результативне професійне навчання суб'єктів кримінального провадження (підвищення кваліфікації), зокрема запровадження міжвідомчих програм підвищення кваліфікації, є ще одним важливим напрямом. Системна цифровізація кримінальної юстиції України протягом останнього десятиріччя трансформувала як реалізацію процесуальних процедур, так і використовувані учасниками кримінального провадження інструменти. Навички роботи з реєстрами та базами даних, електронними носіями інформації, гешування даних та базовий OSINT – вже не специфічні хобі правників, а обов'язковий набір знань для детектива, дізнавача, слідчого, прокурора, судді та адвоката. Вказане створює нові виклики для правничої освіти загалом та системи підвищення кваліфікації правників зокрема [126, с. 939].

Практика правозастосування поступово напрацьовує нові підходи для пошуку інформації, виявлення й фіксації доказів електронної форми проте цей процес потребує пришвидшення, систематизації та уніфікації підходів. Досі немає консолідованої концепції організації навчання працівників органів кримінальної юстиції сучасним процесуально-цифровим компетентностям. Йдеться, зокрема, про збір доказів електронної форми, роботу з державними реєстрами та базами

даних, кібербезпеку, роботу із криптовалютою та опановування іншими навичками.

Важко не помітити, що система кримінальної юстиції залишається доволі інертною, в той час як відбулася фактично інформаційна революція, що змушує ґрунтовно переглянути наявні підходи до розслідування кримінальних проваджень. Міжнародна та вже й національна практика правозастосування поступово напрацьовують нові підходи для пошуку інформації, виявлення й фіксації доказів електронної форми проте цей процес вимагає пришвидшення, систематизації та уніфікації підходів.

Це саме та ситуація, коли проблема полягає не стільки й не тільки у недосконалості законодавства, а більшою мірою у необізнаності правоохоронців щодо можливостей, які відкриваються в таких умовах. Проблемою є й відсутність єдиного бачення у практиків – слідчих, прокурорів та суддів – щодо процедури фіксації здобутої інформації, яка дозволить отримувати належні та допустимі докази. За таких умов для адаптації системи кримінальної юстиції важливо започаткувати кілька важливих кроків. По-перше, має відбуватись постійний аналіз найкращих світових та національних практик напрацювання ключових підходів (стандартів) збирання та фіксації доказів електронної форми. По-друге, слід зробити систематичним обмін досвідом і навчання фахівців системи кримінальної юстиції. Очевидно, обидва напрями можуть бути поєднані шляхом формування міжвідомчих експертно-тренерських команд та осередків формування практик роботи з електронними джерелами [126, с. 940].

Г. Авдєєва, Е. Живуцька-Козловська (2023) зазначають, що оскільки від компетенції та правильного рішення працівників правозастосовних органів залежить, чи відіграватиме окремий цифровий доказ провідну роль у вирішенні конкретної справи, вони мають знати базові технологічні характеристики цифрових пристроїв і цифрової інформації. Тож слід розробити відповідну методичну й довідкову літературу та додати її до програм підвищення кваліфікації окремо для кожної категорії таких співробітників [4, с. 141].

Сьогодні Тренінговий центр прокурорів України вже зорганізував команду небайдужих до тематики фахівців із прокуратури, НАБУ, кіберполіції та громадського сектору, котрі впродовж останніх чотирьох років на підставі власних практичних напрацювань сформували алгоритми пошуку інформації та фіксації доказів, підходи до інформаційної безпеки, роботі з криптовалютою тощо. Тренерсько-експертна команда Тренінгового центру прокурорів України розробила кілька навчальних програм, що мають надзвичайну популярність у прокурорів, і спостерігається бажання інших практиків долучитись до неї. Тобто наразі є вже непогана відправна точка. Безперечно, важливо навчати як тих, хто самостійно застосовуватиме цифрові інструменти, так і тих, хто прийматиме рішення щодо подальшого використання отриманої інформації та доказів електронної форми: оперативних працівників, слідчих, детективів, прокурорів та суддів. У перспективі – й адвокатів також для забезпечення єдиних підходів всієї системи кримінальної юстиції [126, с. 940-941].

За результатами проведеного нами опитування суб'єктів кримінального провадження встановлено, що 68% опитаних не вважають достатніми свої знання щодо доказів електронної форми, 10% вважають, що їх знання в цій сфері потребують покращення та лише 22% респондентів вважають достатніми свої знання щодо доказів електронної форми. При цьому 39% опитаних зазначають, що вони вже проходили навчання / тренінги / підвищення кваліфікації з питань доказів електронної форми, 61% таке навчання не проходили.

Характерним є те, що серед респондентів, які вважають достатніми свої знання, лише половина раніше проходила навчання, тобто інша половина (2/3 з яких є прокурорами) або є дуже технічно освіченими загалом, або не потребують відповідних навичок з огляду на характер діяльності. При цьому 10% респондентів, що вказують на необхідність покращення своїх знань, попередньо проходили профільне навчання [114, с. 90].

Ідеальний стан справ, якого ми прагнемо досягнути у цій сфері, включає такі 10 складників:

1. Навчають професіонали. Тренінги проводять спеціально відібрані та сертифіковані тренери, що є практиками. Команда тренерів складається з детектива, оперативного працівника, прокурора та судді [126, с. 941];

2. Професійні інструменти навчання. Для формування уніфікованих та ефективних практик експертно-тренерську команду має бути розширено, вона має отримати додаткові інструменти формування стандартів роботи у кіберпросторі. До таких інструментів можна віднести систематичні експертні обговорення в межах «круглих столів», дискусій та конференцій, а головне – формування на базі Тренінгового центру прокурорів України «Cyber Hub» навчально-практичної кіберлабораторії. Остання, за умови належного її оснащення необхідним обладнанням, а також інформаційної підтримки, може використовуватись одночасно як для проведення пошуку інформації та фіксації доказів електронної форми в реальних кримінальних провадженнях, так і для навчання практиків;

3. Міждисциплінарний підхід. За такого підходу навчання включає як вивчення законодавчих вимог та процесуальних аспектів, так і технічної складової покрокового проведення конкретних процедур. Такий підхід дозволить синхронізувати бачення оперативних працівників, слідчих / детективів, прокурорів, суддів та технічних експертів у цифровій сфері [126, с. 941]. Одночасне вивчення законодавчих вимог і процесуальних аспектів роботи (наразі це вже реалізовано під час навчання прокурорів щодо доказів електронної форми в кримінальному процесі), а також технічного компонента проведення певних діджитал-процесів [111, с. 48];

4. Тренінговий формат є загальновизнаним ефективним методом навчання дорослих, що володіє очевидними перевагами, порівняно зі стандартними академічними формами навчання. Доцільно організувати професійне навчання, спрямоване на відпрацювання конкретних практичних навичок на основі сучасних інтерактивних підходів роботи із аудиторією. Навчання включатиме навчальні симуляції щодо пошуку інформації, проведення імпровізованих слідчих дій (обшук, огляд комп'ютерів, телефонів, гаманців криптовалюти тощо), відтворення

судових засідань із презентацією прокурором доказів електронної форми аналізом судової практики тощо [111, с. 47-48];

5. Комбінована форма навчання. Офлайн навчання може поєднуватись з онлайн сесіями на платформі ZOOM та проходженням окремих модулів на порталі дистанційного навчання Тренінгового центру прокурорів України [126, с. 941]. Оптимальною формою отримання знань щодо доказів електронної форми респонденти проведеного нами опитування суб'єктів кримінального провадження називають: очні тренінги – 38%; письмові матеріали (методичні рекомендації, статті тощо) – 23%; онлайн тренінги – 21%; короткі відеолекції – 13%; лекції та семінари – 12% [114, с. 91]. На ці відповіді доцільно зважати, готуючи відповідні навчальні заходи;

6. Послідовне багаторівневе навчання за прогресивною шкалою передбачає розбудову покрокової системи тренінгів, що дозволяє обрати тренінг необхідного рівня складності та поступово розвивати певні компетентності від базових понять до просунутих тем та методик. Пропонується проводити тренінги різного рівня складності: а) базові, що можна опрацювати самостійно на порталі дистанційного навчання; б) спеціалізовані для певної категорії працівників, що реалізуються в онлайн чи офлайн-форматі; в) високоспеціалізовані тренінги, що передбачають спільне навчання представників різних органів кримінальної юстиції виключно в офлайн-форматі [111, с. 49-50];

7. Спільне навчання. Ефективне формування досліджуваних навичок можна забезпечити при формуванні комбінованих груп, до яких входимуть прокурори, судді, слідчі, детективи, оперативні працівники [126, с. 942]. Спільне навчання представників органів кримінальної юстиції є запитом самих учасників тренінгів, а тому неодмінно потребує практичної реалізації. Необхідно розглянути можливість формування спільних груп з суддів, прокурорів, слідчих, детективів, оперативних працівників. Тренінговим центром прокурорів України (за участі автора як одного з тренерів) у співпраці з Національною школою суддів України та Радою Європи (в межах проєктів Ради Європи «HELP (Освіта в галузі прав людини для представників юридичних професій) для України, в тому числі під час війни» [367] та «Cyber UA:

Посилення спроможності з питань електронних доказів у воєнних злочинах та грубій порушення прав людини в Україні» [75]), проведено ряд спільних тренінгів для прокурорів та суддів, результати яких свідчать про високу ефективність такого формату навчання, адже відбувається обмін досвідом, формування спільного бачення актуальних проблем правозастосування, усвідомлення потреб колег з інших органів кримінальної юстиції [111, с. 48-49];

8. Регіональне або кущове формування груп передбачає організацію тренінгів для прокурорів, суддів, слідчих, детективів, оперативних працівників з однієї області чи сусідніх областей (так званого «куща»). Цей підхід дозволить сформувати у представників певної області або регіону спільне бачення актуальної проблеми правозастосування, зрозуміти потреби колег та проблемні питання в їх роботи, знайти «точки дотику» у дискусійних питаннях правозастосування, налагодити міжвідомчу взаємодію [111, с. 49];

9. Навчання мотивованих працівників. Доцільно уникати практик примусового навчання, направлення на навчання за залишковим принципом або запису на тренінги людей без додаткового їх відбору. Відбір для навчання хедлайнерів, аналіз кандидатів (посада, функціональні обов'язки, залученість до роботи з цією категорією злочинів), проведення анкетування тощо;

10. Обмін актуальним досвідом та формування уніфікованих стандартів роботи. Формування системи обміну досвідом між працівниками за темами, створення форумів (наприклад, на порталі дистанційного навчання). Розробка та обмін стандартами роботи та методичними матеріалами: інструкціями, пам'ятками, зразками процесуальних документів, практикою судів тощо [126, с. 942].

Такий комплексний підхід дозволить суттєво змінити якість та ефективність роботи системи кримінальної юстиції в умовах тотальної цифровізації світу.

Одним із важливих напрямів підвищення ефективності роботи з доказами електронної форми у кримінальному провадженні є впровадження уніфікованих методичних підходів для всіх суб'єктів кримінального провадження, залучених до їх пошуку, фіксації, дослідження та оцінки. З огляду на складність технічної природи таких доказів та різноманітність практики їх процесуальної обробки,

відсутність єдиних підходів призводить до фрагментарності, суперечливості, а часом — до втрати або визнання недопустимими.

Питання уніфікації правозастосовної практики є надзвичайно актуальним. Нами встановлено, що практика використання одних і тих же доказів електронної форми в кількох кримінальних провадженнях має місце в роботі 51% респондентів, зокрема 29% вказують на практику дублювання доказів, а 17% — на повторне долучення доказів по справі, також 3% опитаних підтверджують, що відповідне використання супроводжується наданням дозволу суду на використання доказів у іншому провадженні, а ще 2% — на конкретну процесуальну процедуру отримання — тимчасовий доступ до речей і документів — іншої справи, в якій є необхідний доказ. При цьому 48% опитаних зазначають про відсутність подібної практики в їх роботі, а ще 1% складно відповісти на це питання. Очевидно, відповідна практика потребує унормування [114, с. 86]. На цей час є численні національні та закордонні методичні рекомендації у досліджуваній сфері [396; 32; 31; 30; 25; 395; 388].

Очевидно, що неможливо забезпечити єдину практику правозастосування щодо доказів електронної форми в кримінальному процесі України за умови існування численних методичних рекомендацій та практичних посібників. Насамперед суб'єкти кримінального провадження фізично не можуть охопити такий обсяг методичних матеріалів. Як наслідок, вивчаються та використовуються різні матеріали з різними підходами, що уможливорює дисбаланс та неоднорідність практики правозастосування.

За результатами фінального обговорення учасниками Круглого столу з питань електронних доказів у кримінальному процесі України, що відбувся 28-29 січня 2025 року в м. Києві, організований Тренінговим центром прокурорів України, Проєктом Ради Європи Cyber UA, Консультативною місією Європейського Союзу з реформування сектору цивільної безпеки України та Національною школою суддів України, сформульовано пропозиції щодо створення загальних базових стандартів роботи з доказами електронної форми під час кримінального провадження, що включають: а) узагальнені, уніфіковані та засновані на вимогах КПК України правила роботи з доказами електронної форми

під час кримінального провадження; b) такі, що допускають можливість деталізації окремих положень; c) містять особливості поводження щодо: носіїв інформації; технічних пристроїв; інформації з відкритих джерел / кіберпростору; криптовалюти.

У цьому контексті важливим інструментом є розроблення СОП, що виступають формалізованим описом послідовності дій, які мають бути вчинені суб'єктами кримінального провадження у типових ситуаціях, пов'язаних із доказами електронної форми. Їхнє головне призначення полягає у забезпеченні передбачуваності та повторюваності дій, що унеможлиблює випадкові відхилення та сприяє формуванню допустимої доказової бази. Важливо підкреслити, що СОП не повинні мати нормативно-правового характеру. Їх доцільно закріплювати як міжвідомчі методичні рекомендації, що приймаються спільно правоохоронними та судовими органами та узгоджуються на міжвідомчому рівні. Такий формат дозволить забезпечити їх гнучкість і динамічність, що важливо у сфері ІТ, де розвиток технічних засобів та методів є надзвичайно швидким. Основними завданнями СОП мають бути: формування єдиної термінологічної та методичної бази у сфері кримінального процесу, пов'язаного з доказами електронної форми; доступний виклад процедур пошуку та фіксації доказів електронної форми як синтезу норм КПК України та ДСТУ ISO/IEC 27037:2017; формулювання загальних рекомендацій до використання технічних засобів та ПЗ; визначення порядку взаємодії між слідчим, прокурором, спеціалістом та експертом під час роботи з доказами електронної форми; запровадження єдиних критеріїв оцінки цілісності, достовірності та допустимості таких доказів; формулювання загальних рекомендацій до дослідження доказів під час судового розгляду тощо.

Запровадження СОП сприятиме забезпеченню єдності правозастосовної практики поводження з доказами електронної форми незалежно від територіальної юрисдикції чи відомчої належності. Окрім того, СОП виконуватимуть превентивну функцію, знижуючи ризик визнання доказів недопустимими через порушення процесуальних правил або технічних вимог. З урахуванням міжнародного досвіду, СОП повинні розроблятися з опорою на ДСТУ ISO/IEC 27037:2017, а також із

урахуванням практики ЄСПЛ щодо допустимості доказів. Це дозволить забезпечити відповідність української моделі міжнародним орієнтирам і підвищить рівень легітимності використання таких доказів під час судового розгляду.

Таким чином, стандартизація підходів шляхом розробки СОП виступає не альтернативою законодавчому регулюванню, а його важливим інституційним доповненням, спрямованим на уніфікацію та підвищення ефективності практики роботи з доказами електронної форми. СОП мають стати інструментом забезпечення передбачуваності, послідовності та правової визначеності у діяльності суб'єктів кримінального провадження, водночас зберігаючи достатню гнучкість для адаптації до швидкозмінних умов цифрового середовища.

Міжвідомча взаємодія у сфері роботи з доказами електронної форми потребує розширення змісту кожного з наявних векторів співпраці та їх прив'язки до реальної процесуальної логіки КПК України і технологічних стандартів цифрової криміналістики.

По-перше, співпраця органів досудового розслідування та прокуратури має виходити за межі формального процесуального керівництва і містити спільне планування способів пошуку та фіксації доказів електронної форми що включає, наприклад, вибір між фізичним вилученням електронних носіїв інформації або інформаційних систем і криміналістичним (побітовим) копіюванням даних (під час огляду, обшуку, тимчасового доступу до речей і документів) з обов'язковим залученням спеціаліста, а також попередню оцінку підстав і пропорційності подолання систем логічного захисту для отримання доступу до даних. Така взаємодія має спиратися на алгоритмізований підхід до прийняття рішень під час обшуку та огляду, дотримання послідовності «ідентифікація – збирання – здобуття – збереження» за ДСТУ ISO/IEC 27037:2017 і забезпечення безперервного документування chain of custody, що прямо кореспондує із вимогами допустимості та достовірності доказу. Додатково прокурор повинен контролювати дотримання процесуальних вимог під час копіювання доказів електронної форми в контексті ч. 4 ст. 99 КПК України, за якою виготовлена копія прирівнюється до оригіналу

документа, що зумовлює підвищені вимоги щодо залучення спеціаліста, якості технічних дій і процесуальної форми їх відображення.

По-друге, залучення технічних фахівців має бути не епізодичним, а інтегрованим у роботу з доказом – від моменту виявлення до дослідження під час судового розгляду. Предметом взаємодії з технічними фахівцями є не лише дії спеціаліста чи висновок експерта, а й криміналістично «чисте» здобуття даних: створення повних криміналістичних (побітових) копій, фіксація геш-сум, робота з оперативною пам'яттю, коректний та детальний опис у протоколах слідчих (розшукових) дій застосовуваних інструментів і методів тощо. Саме технічні фахівці забезпечують відтворюваність технічних процедур, сумісність з міжнародними підходами та можливість подальшої незалежної перевірки, що особливо важливо, коли фізичне вилучення систем обмежене законодавчо або технічно недоцільне, а копіювання є єдиним пропорційним способом збирання доказів електронної форми.

Науковці переконані, що для усунення недоліків (помилки), пов'язаних з проведенням слідчих (розшукових) дій під час розслідування злочинів даної категорії і призначенням експертизи комп'ютерної техніки та програмних продуктів, які ускладнюють або унеможливають проведення такої експертизи, потрібні комплексні заходи, серед яких необхідність необхідність: за можливості до призначення експертизи провести огляд об'єктів із залученням фахівця в галузі використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Такий огляд дасть змогу встановити наявність даних, що можуть мати доказове значення у кримінальному провадженні та загалом вирішити питання доцільності призначення експертизи; узгодження переліку питань за конкретними об'єктами з відповідними фахівцями, оптимізація кількості таких питань та об'єктів, які надаються на експертизу; нормативно-правове закріплення різновидів судових експертиз, які проводить Експертна служба МВС України, визначення питань, які вони можуть вирішити, а також вимог до наданих на експертизу матеріалів; розроблення окремого порядку залучення вузькопрофільних спеціалістів (судових експертів) до виконання

традиційних експертиз, що безпосередньо не пов'язані з дослідженнями комп'ютерної техніки, але в процесі їх проведення виникає потреба в вивченні електронних носіїв інформації та (або) інформаційних слідів на віддалених пристроях збереження даних, серверах, хмарних сховищах тощо [267].

По-третє, координація дій з суб'єктами, що володіють критичною технічною інфраструктурою та унікальними для слідства даними: провайдерами електронних комунікаційних послуг, банківськими установами, хмарними сервісами, криптобіржами тощо; має набути регламентованого й уніфікованого характеру. Вона повинна враховувати законодавчі обмеження, однак також повинна відповідати сучасним підходам цифрового середовища.

Як ніколи до того, нині нагальною є потреба в модернізації процедури здійснення тимчасового доступу до речей і документів. Існуюча практика його реалізації, особливо у випадках роботи з цифровими даними, демонструє значну невідповідність сучасним вимогам.

На практиці, механізм виконання тимчасового доступу до речей і документів в частині доступу до даних операторів телекомунікації на сьогодні реалізується шляхом особистого прибуття слідчого або прокурора (визначеного в ухвалі про тимчасовий доступ до речей і документів) до оператора телекомунікації, передавання оригіналу ухвали та носія інформації (як правило це оптичний диск) для запису запитуваних даних, очікування в черзі разом з колегами та отриманні носія інформації з даними. При цьому офіси ключових операторів телекомунікації територіально розташовані в м. Київ, що вимагає фізичного прибуття уповноважених в ухвалі осіб з усіх куточків держави. У практиці органів досудового розслідування з територіально відділених регіонів є практика підготовки всіх клопотань досліджуваного характеру з визначенням уповноваженої особи за одними і тими ж слідчими, після чого накопичується певна кількість цих ухвал та слідчий особисто їде до м. Києва, де передає відповідні ухвали представнику оператора телекомунікації (залишає власні контактні дані та домовляється про повідомлення його про готовність запитуваної інформації). Після цього слідчий повертається до місця своєї служби та очікує на дзвінок

представника оператора телекомунікації. Для отримання запитуваних даних слідчий знову їде до м. Київ у офіс оператора телекомунікації, забирає носії інформації з запитуваними даними та везе їх до місця роботи. Тобто слідчий (або ж прокурор) фактично виконує функції кур'єра. Вказане ілюструє витрату величезної кількості часу та матеріальних ресурсів, є вельми формалізованим та вкрай неефективним процесом. Такий паперовий і людський фактор ускладнює і сповільнює процес отримання доказів, особливо коли йдеться про великі обсяги інформації чи про дані, що можуть швидко змінюватися або знищуватися. Показово, що навіть законодавець у надзвичайних ситуаціях змушений спрощувати процедуру: зокрема, в умовах воєнного стану для окремих категорій даних дозволено надання тимчасового доступу до речей і документів на підставі постанови прокурора (за погодженням з керівником органу прокуратури) замість ухвали судді, що підкреслює важливість оперативності реалізації цього заходу забезпечення кримінального провадження.

Теперішній механізм реалізації виглядає архаїчним з огляду на сучасний рівень цифрового розвитку держави, зокрема в умовах функціонування Єдиної судової інформаційно-телекомунікаційної системи, до якої інтегровано підсистему «Електронний суд». Звернення з клопотанням до суду про тимчасовий доступ вже відбувається через зазначену підсистему, однак етап виконання відповідної ухвали залишається поза межами електронного документообігу. На нашу думку, оптимізація цього процесу має відбуватись шляхом створення єдиного технічного рішення – платформи (або модуля), інтегрованого в інформаційні системи операторів телекомунікації, що дозволить забезпечити скерування до операторів телекомунікації ухвал про тимчасовий доступ в електронній формі. Така платформа має функціонувати як проміжна захищена ланка, до якої надходитимуть ухвали слідчих суддів, підписані КЕП, супровідні листи слідчих або прокурорів, а також – запитувані матеріали (цифрові дані) в зашифрованому вигляді. Важливо наголосити, що реалізація зазначеного механізму не потребує внесення змін до КПК України. Його впровадження можливе на рівні міжвідомчої інструкції та Меморандуму з операторами телекомунікації, які визначають порядок обміну

інформацією, формат електронних документів, алгоритм автентифікації осіб, уповноважених на отримання даних, а також вимоги до захисту даних, особливостей взаємодії сторін. Водночас такий механізм має забезпечити: достовірність отриманих даних через використання алгоритмів гешування та КЕП; захист персональних даних та службової інформації; спрощення та уніфікацію процесу виконання ухвал по всій території України; мінімізацію людського чинника та уникнення фізичних контактів, які уповільнюють процедуру. Отже, у межах чинного правового регулювання існують всі передумови для формування сучасного електронного механізму реалізації тимчасового доступу до речей і документів, що перебувають у володінні телекомунікаційних операторів телекомунікації.

Розроблений нами підхід до цифровізації механізму виконання ухвал слідчого судді про тимчасовий доступ до речей і документів у частині даних операторів телекомунікації узгоджується із міжнародно-правовими зобов'язаннями України, зокрема з положеннями Конвенції про кіберзлочинність, та Другого додаткового протоколу до неї. Згідно з п. b ч. 1 ст. 18 Будапештської конвенції кожна Сторона зобов'язана вжити такі законодавчі та інші заходи, які можуть бути необхідними для надання повноважень своїм компетентним органам видавати ордери постачальнику послуг, який пропонує свої послуги на території Сторони – про надання інформації про користувача послуг, пов'язаної з такими послугами, яка знаходиться у власності або під контролем такого постачальника послуг. Пропонована нами модель дозволяє суттєво модернізувати національну процесуальну процедуру, що корелюється з цим положенням.

Крім того, Другий додатковий протокол до Конвенції про кіберзлочинність посилює вимоги до ефективної міжвідомчої та міжнародної взаємодії в частині отримання доказів електронної форми зокрема, передбачає можливість прямих запитів до постачальників послуг у транскордонному контексті, що потребує існування технічно організованих, автоматизованих механізмів обміну даними. Аналогічна логіка може і повинна застосовуватись на внутрішньодержавному рівні для досягнення відповідної швидкості та ефективності розслідування. До того ж,

створення єдиного програмного модуля, який дозволить здійснювати передачу ухвал суду та отримання даних в електронному форматі, зможе забезпечити швидкість, достовірність, захищеність, мінімізувати бар'єри до отримання доказів електронної форми. Запровадження запропонованої моделі в межах внутрішнього процесуального механізму не лише сприятиме дотриманню зобов'язань України як Сторони Конвенції про кіберзлочинність, а й формуванню уніфікованого підходу до взаємодії органів досудового розслідування з операторами телекомунікації, що є важливою передумовою для подальшої інтеграції в систему європейського правосуддя.

З урахуванням наведеного, розширена модель міжвідомчої взаємодії повинна бути побудована на трьох опорах: спільне процесуально-технічне планування дій слідчого і прокурора з раннього етапу з урахуванням алгоритмів роботи з доказами електронної форми; інституційно стале інтегроване залучення експертних спроможностей для «чистого» здобуття й збереження даних; стандартизована комунікація з розпорядниками даних і єдині електронні інструменти для документування і передачі результатів.

Розширення практики міжвідомчої співпраці передбачає створення постійно діючих міжвідомчих координаційних платформ. Їхнє завдання полягає у виробленні спільних методичних підходів до роботи з доказами електронної форми (формування та актуалізацію СОП), у міжвідомчій координації та налагодженні взаємодії.

Також слід розробити організаційні заходи щодо запровадження комплексної системи забезпечення цілісності, конфіденційності та збережуваності доказів електронної форми що включає: запровадження гешування як механізму підтвердження цілісності доказів електронної форми; електронні процесуальні документи; запровадження практики резервного копіювання доказів досліджуваної категорії, використання надійних електронних носіїв інформації здатних забезпечити довготривале зберігання цифрових даних, криптографічне шифрування даних (щоб неможливо було їх відкрити і переглянути сторонньому спостерігачу навіть якщо вдасться їх отримати – в контексті забезпечення вимог ст.

222 КПК України); створення відомчих сховищ цифрових даних, інтегрованих у систему контролю доступу з обов'язковим журналюванням усіх дій відповідно до принципів chain of custody.

Отже, організаційні засади удосконалення роботи з доказами електронної форми вимагають комплексного і багаторівневого підходу, спрямованого на підвищення інституційної спроможності системи кримінальної юстиції. Поєднання заходів у сфері освіти, спеціалізації, інфраструктури, навчання, стандартизації, міжвідомчої координації та гарантування цілісності цифрових даних створює архітектоніку цифрової трансформації кримінального процесу в частині роботи з доказами електронної форми.

Важливою передумовою є модернізація правничої освіти та формування нової моделі підготовки кадрів, що поєднує фундаментальну правову базу з технологічними компетентностями. Запровадження профільної спеціалізації слідчих і прокурорів покликане підвищити якість розслідування, а створення криміналістичних ІТ-лабораторій — забезпечити технічну автономність і об'єктивність дослідження цифрових даних. Систематичне професійне навчання та міжвідомчі програми підвищення кваліфікації формують навички роботи з доказами досліджуваної категорії та створюють основу для уніфікованої практики.

Першорядним елементом організаційного вдосконалення є стандартизація: розроблення СОП, здатних забезпечити послідовність і передбачуваність дій суб'єктів кримінального провадження, мінімізувати ризики та втрати доказів чи визнання їх недопустимими. Розширення міжвідомчої співпраці та створення постійно діючих координаційних платформ дозволяє інтегрувати практичний досвід, забезпечити узгодженість процесуальних і технічних підходів, а також налагодити ефективну взаємодію з розпорядниками критичної цифрової інформації. Врешті-решт, створення комплексної системи забезпечення цілісності, конфіденційності та збережуваності доказів із застосуванням процесів гешування, криптографічного шифрування, електронних процесуальних документів і відомчих сховищ цифрових даних формує фундамент для ефективного використання таких доказів у кримінальному процесі.

5.2. Шляхи вдосконалення процесуального регулювання використання доказів електронної форми у кримінальному процесі України

Як вже йшлося, розвиток цифрових технологій та їх глибоке проникнення у сферу кримінального провадження вимагає системного оновлення кримінального процесуального законодавства України. У фокусі цього оновлення мають перебувати положення щодо нормативного закріплення правової природи, статусу та процесуального режиму роботи з доказами електронної форми.

Пропозиції внесення змін до КПК України відносно доказів електронної форми повинні враховувати баланс між прагненням забезпечити впровадження найкращих світових практик роботи з ними та сучасним станом кримінальної процесуальної діяльності в Україні. Науковці і законотворці вже сьогодні спроможні, спираючись на закордонний та міжнародний досвід, підготувати законопроект, який би відображав передові підходи, забезпечував високий рівень підтвердження цілісності цифрової інформації та гарантував незмінність даних упродовж усього кримінального провадження. З наукового погляду, це реальний шлях розв'язання наявних проблем і дієвий механізм упровадження найкращих практик правозастосування — закріпити їх у КПК України як імперативні норми, обов'язкові для виконання органами досудового розслідування та прокурором і врахування суддею при оцінці доказів.

Водночас у цій площині виникає проблема практики правореалізації. Адже далеко не у всіх кримінальних провадженнях ці найкращі практики вже нині реалізовані, а якщо відверто, то лише в поодиноких випадках. Тож у разі імплементації відповідних пропозицій постане ситуація, коли в десятках, а можливо і сотнях тисяч кримінальних проваджень, досудове розслідування яких триває або які перебувають на стадії судового розгляду, будуть наявні докази електронної форми зібрані без дотримання таких високих стандартів. Але ж ці докази фактично використовуються у процесі доказування, і саме на їх основі ухвалюються ті чи інші судові рішення. Тому, вважаємо, закріплення в КПК України пропонованого правового регулювання є передчасним. Однак можливо

реалізувати поетапний, так званий «м'який шлях», який на практиці здійснюється вже понад десять років. Першим етапом такого поступового руху має стати навчання суб'єктів кримінального провадження та розширення їх знань щодо технічних аспектів роботи з доказами електронної форми. Паралельно формується судова практика вищих судів та поступово вносяться точкові зміни до КПК України – цей процес вже спостерігаємо. Наступними кроками є: а) розроблення та впровадження СОП; б) спеціалізація дізнавачів, слідчих, детективів і прокурорів; в) уніфікація судової практики вищими судами; г) системне навчання всіх суб'єктів кримінального провадження базовим поняттям і процедурам; д) внесення змін до КПК України. На нашу думку, реалізація цього етапу з урахуванням поточної ситуації можлива впродовж двох років. І фінальним етапом має стати внесення змін до КПК України щодо закріплення передових світових практик – вимог щодо обов'язкового підтвердження цілісності всіх доказів електронної форми (за допомогою математичних алгоритмів), що використовуються під час кримінального провадження та забезпечення їх chain of custody на всіх етапах кримінального провадження (див. Додаток І). Також доцільно розглянути перспективу врегулювання питання автентичності та цілісності доказів досліджуваної категорії в ГПК України, ЦПК України та КАС України (див. Додаток І).

Позаяк законодавчі зміни в цьому напрямі все ж потрібні зараз, визначимося з основними їх напрямками. Передусім варто вказати, що у процесі вдосконалення кримінального процесуального законодавства щодо роботи з доказами електронної форми необхідно зберегти баланс між формалізацією відповідних процедур і забезпеченням їх ефективності та спроможності в реальних умовах. Надмірна зарегульованість, що виражається у встановленні надто деталізованих вимог до технічного процесу ідентифікації, збирання, здобуття, збереження, аналізу та використання доказів досліджуваної категорії, може створити чимало процесуальних ризиків. Одним із основних негативних наслідків надмірної формалізації є перетворення технічних інструментів правозабезпечення (наприклад, таких як гешування) з гарантій цілісності на підстави для

дискредитації доказу у разі найменшого відхилення від встановленого алгоритму. У цьому разі сутність доказу поступається його формі. Ці ризики особливо відчутні в умовах обмеженості технічного оснащення органів досудового розслідування та недостатнього рівня цифрової компетентності суб'єктів кримінального процесу. Таким чином, надмірна технічна деталізація, не підкріплена адекватним технічним та кадровим забезпеченням, а також формалізований підхід без урахування фактичних можливостей правозастосовних органів може трансформуватися у загрозу штучного нівелювання доказів через технічні порушення. Тому потрібне гнучке нормативне регулювання, що дозволяє адаптуватися до наявних ресурсів.

У зв'язку з цим актуальним є формулювання нормативної конструкції, що ґрунтується на принципі достатності, а не абсолютної технічної відповідності. Це означає, що належне документування доказу електронної форми, може визнаватися допустимим за умови дотримання основних (базових) вимог, що гарантують незмінність, автентичність та простежуваність інформації, навіть за відсутності окремих формальних атрибутів. Законодавство повинно надати суду дискреційні повноваження щодо оцінки доказів електронної форми на основі змістовного, а не винятково формального критерію, із урахуванням специфіки конкретного провадження, умов збирання та рівня технічного забезпечення.

Отже, щоб уникнути цих ризиків, доцільно впровадити гнучкий, адаптивний правовий підхід, що передбачає поступове унормування практики використання доказів електронної форми в кримінальному провадженні, встановлення обов'язкових мінімальних стандартів технічного оформлення та створення умов для поетапного підвищення кваліфікації суб'єктів кримінального процесу. Такий підхід забезпечує не лише відповідність сучасним технічним реаліям, а й гарантує збереження балансу між правовою визначеністю, процесуальними гарантіями та фактичними можливостями на практиці.

Зауважимо, що пропозиції щодо внесення змін до КПК України є гострою дискусійною темою серед науковців і практиків. Тож доречно викласти тут наші міркування про зміни кримінального процесуального закону в частині врегулювання роботи з доказами електронної форми. Першорядним напрямом

удосконалення вважаємо уніфікацію термінології. У чинному КПК України немає базових дефініцій «електронний носій інформації» чи «комп'ютерні дані», що призводить до неоднозначного тлумачення відповідних норм та створює труднощі у правозастосуванні. Доцільно закріпити у КПК України ці поняття шляхом імплементації термінів, закріплених у Конвенції про кіберзлочинність, зокрема «комп'ютерна система» та «комп'ютерні дані», що сприятиме гармонізації внутрішньодержавних норм із міжнародними зобов'язаннями України.

У ст. 84 КПК України визначено види процесуальних джерел доказів. З метою усунення правової невизначеності доцільним видається закріплення на рівні закону того факту, що докази можуть існувати як у матеріальній, так і в електронній формі. Це забезпечить нормативне підґрунтя для інтеграції сучасних форм доказової інформації в єдину систему кримінального процесу.

Пропозиції стосуються і положень ст. 93 КПК України, яка регулює збирання доказів. Варто доповнити її абзацом, що прямо передбачає можливість представлення доказів у вигляді комп'ютерних даних, поряд із речовими доказами та документами. Водночас у нормі має бути закріплений обов'язок сторін забезпечити автентичність та цілісність таких даних. Доповнити ст. 94 КПК України положенням, що під час оцінки доказів суд зобов'язаний враховувати технічні аспекти їх створення, зберігання та перевірки цілісності, якщо йдеться про докази електронної форми. Крім того, слід визначити процесуальні вимоги до дослідження таких доказів під час судового розгляду, що передбачатимуть їх відтворення у судовому засіданні та перевірку автентичності й цілісності за допомогою технічних засобів. Це забезпечить належний рівень достовірності та допустимості доказів досліджуваної категорії у кримінальному провадженні.

Уніфікації поняттєвого апарату та усуненню суперечностей між нормами, що регулюють використання документів у паперовій та електронній формах, сприятиме виключення слова «матеріальний» з ч. 1 ст. 99 КПК України.

Окремої уваги заслуговує пропозиція щодо доповнення КПК України новою статтею 100-1 «Зберігання доказів електронної форми». Її зміст покликаний забезпечити правову визначеність порядку арешту (здобуття, вилучення) та

зберігання даних у цифровому вигляді. У пропонованій нормі доцільно визначити, що здобуття доказів цієї категорії здійснюється шляхом створення точної копії даних або всього вмісту електронного носія інформації. Лише у випадках, коли копіювання неможливе чи існує ризик втрати інформації, вилучається сам ЕНІ. Така конструкція узгоджується з міжнародними стандартами цифрової криміналістики та забезпечує баланс між інтересами слідства і правами власників технічних засобів.

З метою забезпечення належної процесуальної регламентації роботи з доказами електронної форми варто КПК України доповнити окремою статтею, котра визначатиме порядок їх автентифікації та збереження. У такій нормі має бути передбачено можливість застосування гешування, криптографічного шифрування та резервного копіювання як стандартних способів забезпечення цілісності, достовірності та збережуваності даних. Окремого унормування потребує процесуальна форма «криміналістичного (побітового) копіювання», у межах якої необхідно чітко визначити порядок створення копій електронної інформації, застосування технічних засобів write-blocker, розрахунок геш-значень та протоколювання всіх дій. Така деталізація сприятиме уніфікації практики, підвищенню рівня надійності доказів електронної форми та запобіганню сумнівам у їх автентичності.

З метою підвищення рівня захисту доказів досліджуваної категорії у КПК України треба передбачити дещо футуристичну, однак від того не менш цінну ідею використання блокчейн-технологій як інструменту підтвердження цілісності доказів електронної форми. Зокрема, геш-значення таких доказів може зберігатися у спеціалізованих блокчейн-реєстрах, що унеможливить їх зміну чи підміну без відповідного цифрового сліду. Запровадження цього механізму створить додаткову гарантію автентичності та достовірності доказової інформації, а також сприятиме зміцненню довіри до процесуальних процедур, пов'язаних із використанням електронних даних у кримінальному провадженні.

У кримінальному процесуальному законодавстві необхідно закріпити спеціальні положення, що визначатимуть порядок дій у разі пошкодження, втрати

чи зміни доказів електронної форми. Така процедура повинна передбачати документування факту втрати або модифікації даних шляхом складання відповідного технічного акта спеціаліста, а також визначати вплив подібних обставин на їх допустимість та подальшу оцінку судом. Водночас доцільним є встановлення обов'язку сторін виготовляти резервні копії доказів електронної форми з належним підтвердженням їх автентичності й цілісності, що надаватиме їм статус, рівнозначний оригіналам. Це забезпечить належний рівень захисту доказів та мінімізує ризики втрати її процесуальної цінності.

Враховуючи попередню пропозицію, доцільно також закріпити у КПК України процесуальний обов'язок органів досудового розслідування створювати та підтримувати цифрові архіви, що функціонуватимуть як відомчі сховища для збереження доказів електронної форми. Така вимога забезпечить належну організацію обігу електронних даних у кримінальному провадженні, уніфікує порядок їх зберігання та гарантуватиме цілісність і доступність доказів досліджуваної категорії. З метою узгодження кримінального процесу з сучасними цифровими стандартами доречно передбачити у КПК України норми, що врегулюють можливість створення процесуальних документів у вигляді електронних файлів, підписаних КЕП. Необхідним є визначення порядку їх долучення до матеріалів кримінального провадження та зберігання у цифровому архіві. Водночас мають бути встановлені єдині вимоги до електронних протоколів слідчих (розшукових) дій та інших процесуальних документів, включно з їх автентифікацією та довгостроковим збереженням, що забезпечить належну доказову силу таких документів і унеможливить сумніви щодо їх достовірності.

Перспективним напрямом розвитку кримінального процесуального законодавства є запровадження нової слідчої (розшукової) дії «Огляд віртуального середовища». З цією метою главу 20 КПК України пропонуємо доповнити статтею, яка регламентуватиме процесуальний порядок доступу слідчого або прокурора до даних, що зберігаються у хмарних сервісах, електронних кабінетах та соціальних мережах. Важливим є також закріплення базових стандартів Протоколу Берклі, що визначають принципи належної фіксації, автентифікації та збереження цифрової

інформації. Це дозволить сформувати процесуальний механізм огляду даних у віртуальному середовищі та забезпечить їх допустимість як доказів у кримінальному провадженні.

Важливим є врегулювання процесуального статусу результатів OSINT як потенційного джерела доказів у кримінальному провадженні. З метою усунення правової невизначеності пропонуємо у КПК України передбачити окрему слідчу (розшукову) дію «Пошук відомостей у віртуальному середовищі на основі відкритих джерел інформації», що забезпечуватиме документування інформації з відкритих джерел, зокрема соціальних мереж, онлайн-платформ, супутникових карт та інших інтернет-ресурсів, однак не як одноетапної процедури запропонованої попередньо, а як ланцюжка пошукових запитів, спрямованих на пошук інформації, що стосується обставин вчинення кримінального правопорушення. Така слідча (розшукова) дія повинна передбачати вимоги до протоколювання перебігу OSINT із залученням спеціаліста, фіксацію веб-сторінок, скриншотів чи відеозаписів із зазначенням часу, обчислення та фіксацію геш-значень завантажуваних даних та збереження технічних параметрів середовища (IP-адрес, cookies та інших ідентифікаторів). Закріплення відповідної процедури створить процесуальні гарантії достовірності таких даних та унеможливить їх фальсифікацію. Водночас норми ст. 99 КПК України потребують уточнення, що результати OSINT можуть визнаватися джерелом доказів у формі документа за умови дотримання передбаченого порядку їх фіксації та автентифікації.

Одним із основних завдань є імплементація до КПК України визначених статтями 16, 17 Конвенції про кіберзлочинність механізмів термінового збереження комп'ютерних даних, що зберігаються, та тимчасового розкриття даних про рух інформації. Дотепер Україні бракує спеціальних процесуальних механізмів, які б відповідали вимогам зазначених положень. У главі 15 КПК України врегульовано порядок тимчасового доступу до речей і документів, однак ці інструменти не забезпечують належної ефективності, якщо існує ризик втрати або модифікації електронних даних. Саме тому імплементація статей 16 і 17 Конвенції про кіберзлочинність потребує закріплення в КПК України спеціальних

норм, що регламентують процедури збереження цифрової інформації. З метою усунення існуючої прогалини доцільно доповнити кримінальне процесуальне законодавство новою статтею 245-2 «Термінове збереження комп'ютерних даних, які зберігаються, та тимчасове розкриття даних про рух інформації». У цій нормі передбачається право слідчого або прокурора зобов'язати фізичну чи юридичну особу, яка володіє або контролює відповідні дані, забезпечити їх збереження та цілісність протягом визначеного строку. Первісний термін у 90 днів може бути продовжений ще на 90 днів, якщо є у цьому обґрунтована потреба. Пропонована стаття має охоплювати такі категорії інформації: дані про користувача комунікаційних послуг (ідентифікаційні відомості, адреси, номери доступу, інформацію про рахунки та платежі); дані про рух інформації (маршрут, час, дату, тривалість, технічні характеристики комунікації); змістові дані комунікації. Такий підхід відповідає вимогам Конвенції про кіберзлочинність та забезпечує комплексний підхід до процесуального поводження з електронною інформацією.

Важливою гарантією, передбаченою пропонованою нормою, є можливість зобов'язання особи, яка здійснює збереження даних, дотримуватися конфіденційності факту проведення таких процедур упродовж визначеного строку. Це відповідає принципу мінімального втручання в права суб'єктів та одночасно забезпечує ефективність досудового розслідування. Крім того, у разі нагальної потреби постанова про збереження даних може містити вимогу про тимчасове розкриття достатнього обсягу інформації про рух даних для встановлення постачальника послуг і маршруту комунікації.

У науковій літературі та експертному середовищі зазначається, що відсутність спеціальних судових ордерів на збереження даних фактично унеможлиблює належне виконання міжнародних зобов'язань України. Запровадження нової статті 245-2 дозволить сформувати внутрішньодержавний механізм, сумісний із положеннями Конвенції про кіберзлочинність, забезпечить правову визначеність для суб'єктів кримінального провадження. Слід наголосити, що обсяг таких ордерів має обмежуватися лише наявними даними, що вже зберігаються у комп'ютерних системах. Це узгоджується з концепцією Конвенції

про кіберзлочинність, що не вимагає створення механізму збереження інформації на майбутнє. Водночас передбачене обмеження строку дії ордера (до 90 днів із можливістю продовження) забезпечує баланс між інтересами кримінального судочинства та правами власників даних.

Таким чином, запровадження у КПК України спеціальної норми про термінове збереження комп'ютерних даних сприятиме виконанню міжнародних зобов'язань України, підвищенню ефективності збирання та збереження доказів електронної форми мінімізації ризиків їх втрати або фальсифікації.

Аналіз положень чинного кримінального процесуального законодавства України свідчить про те, що інструментарій, передбачений для отримання інформації, зокрема у сфері електронних комунікацій, є недостатнім для повноцінної імплементації ст. 18 Конвенції про кіберзлочинність. Вказана стаття передбачає можливість застосування судового ордера на представлення інформації як альтернативи обшуку та арешту (вилучення).

У національному законодавстві подібний механізм відображений у главі 15 КПК України, де регламентовано тимчасовий доступ до речей і документів. Проте його конструкція не забезпечує належної визначеності та не відповідає вимогам міжнародного стандарту. По-перше, у законі відсутнє чітке формулювання, яке б охоплювало всі категорії комп'ютерних даних, включно з інформацією про користувача послуг. По-друге, чинна редакція статей 159–165 КПК України не враховує особливостей існування документів та даних в електронній формі, що породжує правову невизначеність і ускладнює практику.

З метою усунення зазначених недоліків доречно внести зміни до статті 160 КПК України, передбачивши право суду за клопотанням прокурора зобов'язати будь-яку фізичну чи юридичну особу надати саме комп'ютерні дані, які перебувають у її володінні або під її контролем, а також зобов'язати постачальників електронних комунікаційних послуг надавати інформацію про користувачів таких послуг. Такий підхід відповідає змісту статті 18 Конвенції про кіберзлочинність, де прямо визначено, що об'єктом ордера на представлення можуть бути будь-які наявні комп'ютерні дані, у тому числі відомості про користувача послуг.

Особливістю імплементації є також можливість надання слідчому або прокурору повноважень у невідкладних випадках самотійно постановляти рішення про витребування інформації про користувача послуг, зокрема в електронній формі. Такий підхід обґрунтовується мінливістю та вразливістю доказів електронної форми, що можуть бути знищені або змінені у короткий проміжок часу. При цьому наявність електронної форми постанови узгоджується з тенденціями цифровізації кримінального провадження та забезпечує оперативність реалізації процесуальних процедур.

Додаткові зміни пропонуємо внести у статті 161–164 КПК України, деталізувавши, що предметом тимчасового доступу можуть бути речі та документи як у матеріальній, так і в електронній формі. Якщо ж ідеться про електронні дані, має бути закріплений принцип пріоритетності отримання їхньої точної копії замість вилучення електронного носія інформації. Лише за умови технічної неможливості створення копії допускається вилучення самого технічного пристрою чи електронного носія інформації. Таке положення є необхідним для забезпечення балансу між інтересами досудового розслідування та правами власників електронних пристроїв.

Своєю чергою, зміни до статті 165 КПК України мають бути спрямовані на спрощення процедури виконання ухвали про тимчасовий доступ, передбачивши можливість її реалізації в електронній формі та автоматизацію процесу передачі даних. Це сприятиме ефективнішому використанню електронних комунікаційних технологій у кримінальному процесі та зменшенню ризиків втрати доказів.

Необхідність таких змін підкріплюється низкою аргументів. По-перше, ордер на представлення інформації є менш інвазивним інструментом порівняно з обшуком і арештом (вилученням), що відповідає принципу пропорційності. По-друге, інформація про користувача послуг має ключове значення не лише для внутрішніх, а й для міжнародних кримінальних розслідувань, де вона часто є первинною ланкою для ідентифікації суб'єктів злочину. По-третє, національне законодавство у поточній редакції передбачає надмірні процесуальні обмеження

для доступу до таких відомостей, що суперечить вимогам визначеності та передбачуваності права.

Отже, імплементація статті 18 Конвенції про кіберзлочинність у кримінальне процесуальне законодавство України вимагає комплексного перегляду норм глави 15 КПК України, зокрема статей 160–165, шляхом закріплення процесуальної можливості отримання електронних даних і відомостей про користувача послуг менш інвазивними процесуальними засобами. Це дозволить забезпечити виконання міжнародних зобов'язань України, підвищить ефективність розслідувань та сприятиме розвитку сучасних підходів до поводження з доказами електронної форми.

Також раціональним є доповнення статей 159–164 КПК України положеннями, які б регламентували можливість виконання ухвал слідчого судді про тимчасовий доступ до речей і документів у цифровій формі через захищений електронний комунікаційний модуль, інтегрований з провайдерами та операторами телекомунікацій. Використання такого технологічного каналу дозволить забезпечити оперативність і безпеку обміну процесуально значущими даними, суттєву економію матеріальних та людських ресурсів, а також зменшити ризики втрати чи спотворення даних. При цьому дані, отримані через зазначений механізм, повинні мати однаковий процесуальний статус із тими, що здобуті традиційним шляхом, що гарантуватиме їхню допустимість і належність як доказів у кримінальному провадженні.

Важливим етапом є гармонізація кримінального процесуального законодавства України з положеннями ст. 19 Конвенції про кіберзлочинність в частині адаптації правил щодо проведення обшуку та арешту (здобуття, вилучення). Стаття 19 Конвенції про кіберзлочинність передбачає надання компетентним органам спеціальних повноважень щодо доступу до комп'ютерних систем, їхніх частин або носіїв інформації, а також копіювання даних, забезпечення їхньої цілісності та можливості блокування чи заборони доступу.

Чинні положення КПК України (зокрема статті 233–236, що регулюють обшук і огляд, та статті 167–169 щодо тимчасового вилучення майна) були

сконструйовані переважно для матеріальних об'єктів. Попри те, що законодавець уже врахував у низці статей можливість поводження з інформацією в електронній формі, застосування загальних правил щодо «майна» чи «документів» виявляється недостатнім у контексті цифрових даних, які мають специфічні властивості: мінливість, залежність від технічного середовища та вразливість до втрати або модифікації.

З метою забезпечення відповідності національного законодавства ст. 19 Конвенції про кіберзлочинність пропонується конкретизувати процесуальні положення щодо обшуку та огляду комп'ютерних систем. Йдеться про закріплення можливості у невідкладних випадках (зокрема коли існує загроза втрати чи спотворення електронних даних) проводити проникнення до житла чи іншого володіння особи для виявлення та фіксації комп'ютерних даних.

Окремого унормування потребує питання вилучення електронних носіїв інформації або їх частин. Важливим є закріплення пріоритету копіювання даних над вилученням обладнання. Лише у разі технічної неможливості створення точної копії має здійснюватися вилучення комп'ютерної системи чи електронного носія інформації.

Додатково варто передбачити процесуальний обов'язок фіксації у протоколах обшуку та огляду причин вилучення технічних пристроїв замість копіювання даних. Такий обов'язок забезпечить належний рівень процесуального контролю і сприятиме дотриманню принципу пропорційності при обмеженні прав власників комп'ютерних систем.

Упевнені, що внесення запропонованих змін дозволить: повноцінно поширити дію процесуальних інститутів обшуку та арешту (здобуття, вилучення) на сферу доказів електронної форми; надати компетентним органам інструменти для копіювання, збереження та блокування даних відповідно до вимог міжнародних стандартів; забезпечити баланс між ефективністю досудового розслідування та гарантіями прав осіб, щодо яких здійснюються процесуальні дії; усунути правову невизначеність у сфері застосування традиційних процесуальних заходів щодо електронних даних.

Отже, імплементація ст. 19 Конвенції про кіберзлочинність в національне кримінальне процесуальне законодавство України потребує комплексного перегляду положень, що регламентують обшук, огляд та арешт, із метою створення правового підґрунтя для належної роботи з доказами електронної форми.

З метою належного врегулювання ситуацій, коли існує високий ризик втрати електронних даних, слід доповнити статті 233–237 КПК України положеннями щодо процедур невідкладного доступу до інформації, що має електронну форму, зокрема даних оперативної пам'яті чи онлайн-комунікацій. Такий доступ може здійснюватися без попередньої ухвали слідчого судді лише у випадках безпосередньої загрози знищення або модифікації даних, за аналогією до інституту «невідкладного обшуку». При цьому повинні бути встановлені чіткі часові межі проведення експрес-огляду, обов'язкове протоколювання дій та подальший судовий контроль для підтвердження законності отримання таких доказів. Це забезпечить баланс між потребами оперативного реагування та гарантіями захисту прав учасників кримінального провадження.

Щоб забезпечити баланс між потребами досудового розслідування та безперервністю господарської діяльності варто окремо передбачити у КПК України спеціальні положення щодо порядку вилучення серверів та корпоративних інформаційних систем. Зокрема, орган досудового розслідування повинен бути зобов'язаний у першу чергу здійснювати копіювання необхідних даних із подальшою передачею копій власнику для забезпечення функціонування його діяльності, надаючи пріоритет саме копіюванню перед фізичним вилученням технічних засобів. Окремо має бути чітко визначено недопустимість вилучення серверів та корпоративних інформаційних систем об'єктів критичної інфраструктури, з мотивів забезпечення безпеки та стабільності суспільно важливих процесів.

Важливе значення має імплементація положень Конвенції про кіберзлочинність, які встановлюють баланс між потребами слідства та гарантіями захисту прав людини у сфері приватного спілкування. Насамперед варто переглянути норми ст. 263 КПК України, що регламентує зняття інформації з

транспортних телекомунікаційних мереж. У сучасних умовах ця норма повинна чітко розмежовувати доступ до змісту інформації та до даних про рух інформації. Перший із зазначених видів доступу є більш інвазивним і може здійснюватися виключно за ухвалою слідчого судді за наявності обґрунтованої підозри у вчиненні тяжкого чи особливо тяжкого злочину або злочину. Такий підхід відповідає міжнародним стандартам і гарантує пропорційність втручання у право на приватність.

Паралельно постає потреба у впровадженні нової процесуальної норми – статті 264-1 КПК України «Доступ до інформації про спілкування та її аналіз (дані про рух інформації)». Йдеться про врегулювання порядку доступу до даних про рух інформації у реальному часі, які відрізняються за своїм характером від даних змісту комунікації. Такі відомості мають важливе значення для ідентифікації користувачів комунікаційних послуг, визначення місця розташування пристрою, за допомогою якого здійснюється комунікація, частоти та тривалості контактів. Разом з тим, доступ до цієї категорії даних, як і у випадку зі змістом інформації, повинен відбуватися лише на підставі ухвали слідчого судді.

Закріплення на рівні закону таких положень дозволить диференціювати процесуальні повноваження залежно від характеру даних: зміст комунікаційної інформації або дані про її рух. Це сприятиме дотриманню принципу пропорційності та забезпечить належні запобіжні механізми. Важливо також передбачити обов'язок постачальників послуг забезпечувати технічну можливість доступу до таких відомостей, гарантувати конфіденційність проведення зазначених заходів та вести облік усіх випадків надання доступу для цілей нагляду.

Запровадження запропонованих змін має важливе значення з кількох причин: по-перше, це дозволить забезпечити виконання міжнародних зобов'язань України у сфері протидії кіберзлочинності; по-друге, удосконалення правового регулювання НСРД сприятиме підвищенню ефективності досудового розслідування у справах, пов'язаних з використанням комп'ютерних технологій; по-третє, диференційований підхід доступу до різних категорій інформації

створить умови для належного балансу між завданнями кримінального провадження та захистом конституційних прав громадян.

У сфері НСРД доцільним є також встановлення спеціальних процесуальних вимог до фіксації їх результатів з метою підтвердження автентичності та цілісності отриманої інформації. Для цього у КПК України варто передбачити застосування методів гешування, ведення службових журналів та складання технічних протоколів, що підтверджуватимуть автентичність та цілісність результатів НСРД. Такий підхід створить безумовні гарантії незмінності результатів НСРД як доказів у кримінальному провадженні, що усуне необхідність сторони захисту в з'ясуванні відповідних питань під час судового розгляду.

З огляду на тенденції цифровізації правосуддя доцільним є доповнення КПК України положеннями про цифрову ідентифікацію учасників кримінального провадження. Зокрема, слід передбачити можливість автентифікації слідчих, прокурорів, захисників та інших учасників під час доступу до доказів електронної форми шляхом використання КЕП або, наприклад, засобів системи «Дія. Підпис». Це підвищить рівень процесуальної безпеки та унеможливить несанкціонований доступ до електронних даних. Крім того, варто передбачити аналогічний механізм для цифрової ідентифікації всіх учасників кримінального провадження, що актуально в контексті проведення окремих слідчих (розшукових) дій у дистанційному форматі, зокрема допиту свідка. За умови обов'язкового підтвердження особи учасників такими ж засобами цифрової ідентифікації вказана пропозиція вбачається перспективною. Запровадження відповідних механізмів сприятиме підвищенню ефективності та гнучкості кримінального провадження, зберігаючи при цьому належні гарантії достовірності процесуальних дій.

Одним з актуальних питань є вдосконалення процедури отримання показань під час кримінального провадження за допомогою електронних засобів телекомунікації. У процесі імплементації положення статті 11 Другого додаткового протоколу до Конвенції про кіберзлочинність, дедалі більшої актуальності набуває концепція транснаціонального допиту свідка в режимі онлайн, що передбачає комплексне оновлення процесуального механізму міжнародного співробітництва в

кримінальному провадженні. Йдеться про розроблення змін до КПК України з метою унормування процедури дистанційного допиту свідка, який фізично перебуває в межах юрисдикції іншої держави. Суть запропонованої моделі полягає в тому, що допит здійснюється у режимі відеоконференцз'язку, де ініціатором процесуальної дії виступає правоохоронний орган однієї держави (запитуюча сторона), а технічне та процесуальне забезпечення перебування свідка на території іншої держави (виконуюча сторона) покладається на відповідний орган цієї юрисдикції. При цьому, попри відсутність спільної територіальної юрисдикції, досягається повна правова сумісність і доказова прийнятність результатів такої процесуальної дії у межах внутрішнього кримінального провадження.

Процедурно участь держави перебування свідка полягає у: забезпеченні фізичної присутності свідка в уповноваженому правоохоронному органі (зазвичай – у спеціальному приміщенні, обладнаному засобами відеозв'язку); перевірці його особи на підставі офіційних документів; проведенні ідентифікації (візуальної, можливо – біометричної); забезпеченні контролю за недопущенням будь-якого стороннього впливу на свідка (у тому числі – психологічного або фізичного тиску, погроз чи інших неправомірних дій); наданні технічної підтримки та організації безпечного онлайн-з'єднання з правоохоронним органом держави, що ініціює допит. Безпосереднє проведення допиту здійснюється представником запитуючої сторони – слідчим або прокурором, який перебуває у своїй державі. Такий слідчий отримує від свідка в режимі реального часу усні відповіді на запитання, фіксує зміст показань за допомогою технічних засобів та формує протокол допиту відповідно до норм національного процесуального закону.

Після завершення допиту сформований протокол, який є електронним документом (в розумінні Закону України «Про електронні документи та електронний документообіг»), надсилається уповноваженій особі, яка забезпечує контакт із свідком у державі його перебування. Протокол надається свідку для ознайомлення. За наявності зауважень або доповнень він може бути уточнений, після чого підписується КЕП свідка.

Не менш важливою складовою запропонованої моделі є відеозапис допиту, який виконує функцію додатка до електронного протоколу допиту. Він може супроводжуватись геш-ідентифікатором або іншим засобом автентифікації для підтвердження незмінності запису. Такий відеофайл стає невід'ємною частиною протоколу допиту (додатком), що може бути використаний під час кримінального провадження. Імплементація такої моделі в КПК України забезпечить процесуальну економію, зменшення строків виконання запитів про міжнародну правову допомогу, уникнення екстрадиційних процедур та підвищення доказової цінності показань у справах з транскордонним елементом, зокрема у категоріях кіберзлочинів, наркоторгівлі, торгівлі людьми та транскордонної злочинності загалом.

Особливого врегулювання потребує питання захисту адвокатської та нотаріальної таємниці в електронному форматі. Доцільним видається передбачити у КПК України положення, які б гарантували неможливість необґрунтованого доступу до електронних носіїв, що містять таку інформацію. Як один із можливих механізмів пропонується внесення до Єдиного реєстру адвокатів України відомостей про технічні пристрої, які використовуються адвокатом під час здійснення професійної діяльності та містять адвокатську таємницю. Це дозволить забезпечити додатковий рівень захисту від неправомірного втручання в охоронювану законом таємницю та сприятиме дотриманню принципу недоторканності професійної діяльності адвокатів і нотаріусів.

Необхідним є доповнення статті 290 КПК України положеннями, що закріплюватимуть право сторони захисту на доступ до доказів електронної форми, з належним підтвердженням цілісності відповідних даних. Така зміна забезпечить реалізацію принципу змагальності, гарантуватиме рівність процесуальних можливостей сторін та сприятиме ефективному використанню доказів електронної форми в судовому провадженні. Удосконалення статті 290 КПК України потребує також запровадження чітких гарантій захисту персональних даних і приватності особи. Доцільно передбачити процесуальні механізми, що забезпечуватимуть баланс між завданнями кримінального провадження та правом на повагу до

приватного і сімейного життя, особливо у випадках отримання під час досудового розслідування доступу до електронної пошти, месенджерів, акаунтів у соціальних мережах чи інших персональних даних. Для цього варто закріпити для сторони обвинувачення спеціальну процедуру «процесуального мінімалізму», що передбачатиме можливість відкриття в порядку ст. 290 КПК України лише тих відомостей, що безпосередньо стосуються предмета доказування, без надмірного втручання у приватне життя та надання всієї інформації з пристрою чи облікового запису. Такий підхід сприятиме дотриманню принципу пропорційності та відповідатиме стандартам захисту прав людини у кримінальному провадженні.

З метою забезпечення належного рівня достовірності та захисту доказів електронної форми у КПК України доцільно закріпити процедуру фіксації ланцюга збереження доказів (chain of custody). Такий порядок має передбачати реєстрацію кожного випадку доступу, переміщення чи копіювання доказів електронної форми з фіксацією часу, уповноваженої особи та характеру здійснених дій. Варто визначити можливість автоматизованого ведення такого журналу в електронній формі, що матиме статус процесуального документа. Для підвищення надійності цього механізму доцільно передбачити можливість застосування сертифікованих систем обліку та реєстрації ланцюга збереження доказів, що функціонують на основі інфраструктурно керованих рішень, зокрема технологій розподілених реєстрів (блокчейн). Використання таких систем повинно ґрунтуватися на верифікованості ПЗ, проведенні незалежного аудиту та обов'язковому протоколюванні всіх доступів і змін, що гарантуватиме автентичність та цілісність.

Доцільно запровадити зрозуміле й чітке зобов'язання постачальників послуг зберігати дані про електронні комунікації, створити чіткі правила доступу та використання такої інформації, сформувані відповідні незалежні органи нагляду та законодавчо передбачити, що таку збережену інформацію належить знищувати після завершення періоду збереження. В цьому контексті варто нагадати, що Рада Європи та Європейський парламент прийняли законодавчі акти, які впровадять нову систему збору доказів електронної форми у кримінальних провадженнях в ЄС. Нові правила щодо доказів електронної форми складаються з двох законодавчих

заходів: Регламент (ЄС) 2023/1543 про європейські ордери на надання та збереження доказів електронної форми в кримінальних провадженнях та для виконання покарань, пов'язаних з позбавленням волі, , в рамках кримінального провадження [490, с. 1]; Директива (ЄС) 2023/1544, що встановлює гармонізовані правила щодо визначення уповноважених установ та призначення законних представників з метою збору доказів електронної форми в кримінальних провадженнях [378, с. 1].

З метою забезпечення послідовного застосування правил та надання часу для їх впровадження та дотримання, Регламент застосовується з 18 серпня 2026 року. Директива повинна бути перенесена до національного законодавства держав-членів ЄС до 18 лютого 2026 року. Головною метою нового законодавства ЄС є створення альтернативного – швидшого та ефективнішого – механізму до існуючих інструментів міжнародного співробітництва та взаємної правової допомоги з метою конкретного вирішення проблем, що виникають у зв'язку з мінливим характером доказів електронної форми та аспектом «втрати місця розташування» збережених даних. Регламент встановлює правила, за якими орган держави-члена в кримінальному провадженні може видати європейський ордер на надання доказів або європейський ордер на збереження доказів і тим самим (безпосередньо) зобов'язати постачальника послуг, який надає послуги в ЄС та зареєстрований в іншій державі-члені, або, якщо він не зареєстрований, представлений законним представником в іншій державі-члені, надати або зберегти докази електронної форми незалежно від місця їх зберігання. Директива встановлює правила щодо призначення визначених установ та призначення законних представників певних постачальників послуг, які надають послуги в ЄС, для отримання, виконання та забезпечення виконання рішень та наказів, виданих компетентними органами держав-членів, з метою збору доказів електронної форми в кримінальних провадженнях [529, с. 1].

Наразі стаття 105 Закону України «Про електронні комунікації» містить надто просту правову основу для зберігання даних. Відповідно до п. 2 ч. 8 ст. 105 Закону постачальники послуг повинні зберігати записи про надані електронні

комунікаційні послуги протягом строку позовної давності, визначеного законом (вказане визначено в контексті забезпечення правильності виставлення рахунків за надані електронні комунікаційні послуги) [226, с. 1]. З метою уніфікації правил зберігання електронних комунікаційних даних та забезпечення належних умов їх доступності для потреб кримінального провадження доцільно було б доповнити Закон України «Про електронні комунікації» новою статтею 105-1 «Обов'язки щодо зберігання даних». У такій статті слід закріпити обов'язок постачальників електронних комунікаційних послуг зберігати визначені законом категорії даних у первинному вигляді або у вигляді даних, що обробляються в процесі надання послуг, протягом строку, який не повинен перевищувати 12 місяців. Порядок зберігання має гарантувати можливість їх оперативного надання компетентним органам відповідно до спеціального законодавства.

При цьому законодавець має встановити низку гарантій захисту таких даних, включаючи обов'язкове забезпечення їх належної якості, недопущення випадкового чи незаконного знищення, зміни або розголошення, а також обмеження доступу виключно для уповноважених осіб. По завершенні визначеного строку зберігання дані повинні підлягати знищенню. На постачальників також доцільно покласти обов'язок призначати відповідальну особу з питань інформаційної безпеки, вести облік кінцевих користувачів послуг для їх ідентифікації, розробляти внутрішні процедури виконання передбачених вимог, а також фіксувати інформацію про запити компетентних органів на доступ до даних із зазначенням правової підстави та характеру виданих відомостей. Закріплення вказаних положень забезпечить баланс між потребами кримінального переслідування та гарантіями захисту інформації, а також відповідатиме міжнародним стандартам у сфері електронних комунікацій і кібербезпеки.

З метою нормативного унормування обов'язків постачальників електронних комунікаційних послуг щодо зберігання даних доцільним буде доповнення Закону України «Про електронні комунікації» статтею 105-2 «Категорії збережених даних». У цій статті необхідно закріпити, що обов'язок із збереження, визначений у пропонованій нами вище статті 105-1 цього Закону, охоплює 6 категорій даних

(що корелюються з визначеними у ст. 5 Директиви Європейського Парламенту та Ради 2006/24/ЄС від 15 березня 2006 року про зберігання даних, що генеруються або оброблюються у зв'язку з наданням загальнодоступних електронних комунікаційних послуг або мереж загального користування, та про внесення змін до Директиви 2002/58/ЄС [379, с. 1]): дані, необхідні для відстеження та ідентифікації джерела надсилання повідомлення; дані для ідентифікації адресата; відомості про дату, час та тривалість передання повідомлення; інформацію про тип повідомлення; відомості, що дають змогу ідентифікувати користувачів та їхнє комунікаційне обладнання; дані, пов'язані з ідентифікацією обладнання мобільного зв'язку. При цьому обов'язок збереження поширюється також на дані щодо безрезультатних спроб з'єднання, коли їх збереження прямо передбачене.

Водночас у тексті Закону має бути чітко визначено, що збережені дані не можуть охоплювати відомості, які розкривають зміст повідомлень, оскільки це становило б непропорційне втручання у право на приватність. Деталізований перелік окремих категорій даних доцільно віднести до предмета підзаконного регулювання, що дозволить враховувати технологічні особливості функціонування комунікаційних мереж та забезпечити їх своєчасне оновлення. Закріплення таких положень забезпечить баланс між інтересами кримінального провадження та гарантіями захисту приватного життя, створить необхідні передумови для ефективного використання даних як доказів відповідно до норм КПК України.

Точний перелік категорій даних, що підлягають зберіганню, необхідно встановити у підзаконних актах, прийнятих на основі наведених вище пропозицій щодо доповнення Закону України «Про електронні комунікації» статтями 105-1 та 105-2. Для цієї мети пропонується використати перелік, визначений у ст. 5 Директиви Європейського Парламенту та Ради 2006/24/ЄС від 15 березня 2006 року про зберігання даних, що генеруються або оброблюються у зв'язку з наданням загальнодоступних електронних комунікаційних послуг або мереж загального користування, та про внесення змін до Директиви 2002/58/ЄС [379, с. 1], яка в 2014 році скасована Судом ЄС через порушення нею основних прав, зокрема права на приватність. Попри скасування цієї директиви, нас цікавлять технічні аспекти

категорій даних, що зберігаються. При цьому процедури отримання вказаних даних під час кримінального провадження вбачається необхідним визначити із забезпеченням суворих гарантій права на приватність.

Важливим напрямом удосконалення нормативного регулювання у сфері роботи з доказами електронної форми є розроблення та затвердження міжвідомчого підзаконного НПА, який визначатиме порядок взаємодії органів досудового розслідування, прокуратури та інших компетентних органів із НКП 24/7. Такий акт має стати обов'язковим елементом нормативної інфраструктури, оскільки саме він забезпечить уніфіковані правила співпраці уповноважених органів при реалізації механізмів Конвенції про кіберзлочинність.

Доцільним є розроблення цього міжвідомчого документа за формою, аналогічною до Інструкції про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол 17.08.2020 [229, с. 1]. Вибір такої моделі пояснюється тим, що зазначена Інструкція вже продемонструвала свою ефективність у забезпеченні уніфікованого порядку міжвідомчої взаємодії в умовах міжнародного обміну даними, чітко визначивши суб'єктів, процедури та обов'язки учасників.

З урахуванням специфіки діяльності НКП 24/7 у проєкті міжвідомчого НПА пропонується, серед іншого, зобов'язати суб'єкта, який ініціював звернення до НКП 24/7, надалі невідкладно скеровувати запит про міжнародну правову допомогу щодо витребування збережених даних. Водночас якщо необхідність у подальшому їх зберіганні відпаде, такий суб'єкт має своєчасно інформувати НКП 24/7 про відсутність потреби у продовженні цього заходу. Запровадження таких правил дозволить забезпечити баланс між ефективністю міжнародного співробітництва у сфері протидії злочинності та гарантіями прав учасників кримінального провадження, а також сприятиме ефективній реалізації процедур Конвенції про кіберзлочинність. Кожен з органів досудового розслідування (зокрема СБУ, Національна поліція України, Державне бюро розслідувань, Бюро економічної безпеки України, НАБУ тощо), органи прокуратури, а також судова гілка влади повинні розробити та затвердити власні нормативні акти, що

регулюватимуть питання роботи з доказами електронної форми. Такі акти мають враховувати процесуальну роль відповідного суб'єкта кримінального провадження, особливості організаційної структури відповідного органу та специфіку здійснення його діяльності загалом. Зазначені відомчі акти повинні врегульовувати насамперед питання організаційного характеру, тоді як у частині процесуальних та технічних аспектів доцільним є встановлення відсилочних положень до норм КПК України, положень профільних законів, національного стандарту ДСТУ ISO/IEC 27037:2017, а також до затверджених СОП. Таким чином, розроблення та впровадження відомчих НПА сприятиме уніфікації організаційних механізмів роботи з доказами електронної форми створить належні умови для підвищення ефективності діяльності уповноважених органів та забезпечить їхню відповідність вимогам законодавства і міжнародних стандартів.

Узагальнюючи результати дослідження процесуальних аспектів удосконалення роботи з доказами електронної форми слід констатувати, що розвиток цифрових технологій зумовлює необхідність поетапного та комплексного оновлення кримінального процесуального законодавства України. Запропоновані напрями змін мають забезпечити нормативне закріплення правового режиму доказів електронної форми встановлення мінімальних стандартів їх цілісності й автентичності, а також створення умов для подальшого впровадження передових міжнародних практик. При цьому законодавче регулювання повинно ґрунтуватися на принципі достатності та гнучкості, уникаючи надмірної формалізації технічних процедур. Удосконалення національного кримінального процесуального законодавства має здійснюватися у гармонізації з положеннями Конвенції про кіберзлочинність, Протоколу Берклі та європейських стандартів, із одночасним врахуванням реальних можливостей органів досудового розслідування та судової системи. Таким чином, пропоновані зміни створюють підґрунтя для формування збалансованої та ефективної моделі процесуального поводження з доказами електронної форми здатної гарантувати належний рівень доказової надійності, захист прав учасників провадження та відповідність міжнародним зобов'язанням України.

5.3. Напрями технічного удосконалення використання доказів електронної форми у кримінальному процесі України

В умовах активної цифровізації суспільства кримінальний процес зазнає принципових трансформацій, обумовлених зміною самої природи доказів. У кримінальному провадженні зростає кількість обставин, що підлягають доказуванню на основі даних, що існують у цифровій формі. За таких умов технічна спроможність суб'єктів кримінального процесу щодо належної роботи з доказами електронної форми стає важливим чинником забезпечення ефективної правозастосовної діяльності.

Забезпечення органів досудового розслідування, прокуратури та суду релевантними технічними й програмними засобами є обов'язковою умовою належної роботи з доказами електронної форми.

Мінімально необхідне технічне забезпечення має включати: сертифіковані електронні носії інформації для збереження та передачі доказів електронної форми; пристрої для відеофіксації слідчих (розшукових) дій, інтегровані з системами захищеного зберігання; програмні засоби для створення цифрових протоколів слідчих (розшукових) та процесуальних дій із застосуванням КЕП як слідчими, прокурорами, так і учасниками кримінального провадження; інструменти для гешування та перевірки цілісності цифрових файлів; програмні модулі для верифікації КЕП, електронної позначки часу та контролю цілісності доказів електронної форми; пристрої типу write-blocker, що унеможливають зміну даних на оригінальних носіях під час їх дослідження чи копіювання тощо.

Необхідною умовою функціонування зазначеної інфраструктури є уніфікація технічних і програмних вимог на рівні державної політики та міжвідомчої нормативної бази. Йдеться про розроблення та затвердження мінімальних стандартів обладнання й ПЗ, а також обов'язкову сертифікацію засобів, що застосовуються у кримінальному провадженні. Запровадження таких стандартів забезпечить процесуальну однорідність у діяльності різних органів досудового розслідування, прокуратури та судів, а також унеможливить використання

технічних засобів, які не гарантують автентичності та цілісності цифрової інформації.

Важливою складовою технічного забезпечення є спеціалізовані програмні засоби, призначені для роботи з доказами електронної форми. До них належать: програмні рішення для криміналістичного копіювання цифрової інформації з фіксацією геш-значень; інструменти для аналізу метаданих, електронних журналів подій, мережевих логів; програмні комплекси для відновлення видалених або пошкоджених даних; захищені системи цифрового архівування доказів з можливістю контролю доступу та ведення електронного журналу, що фіксуватиме ланцюг збереження доказу (chain of custody); платформи для проведення судових експертиз у сфері комп'ютерних технологій, які відповідають міжнародним стандартам тощо.

До переліку спеціалізованого ПЗ доцільно включити системи автоматичного журналювання доступу. Такі системи забезпечують фіксацію усіх дій, пов'язаних із переглядом, копіюванням, переміщенням чи модифікацією доказів електронної форми із зазначенням часу, ідентифікатора користувача та характеру здійсненої операції. Застосування автоматизованих журналів доступу створює додатковий рівень гарантій дотримання принципів автентичності та цілісності доказів електронної форми а також підвищує прозорість і контрольованість процесу їх використання. Наявність такого інструменту відповідає вимогам кримінального процесуального законодавства щодо забезпечення належного процесуального оформлення доказів та сприяє реалізації концепції ланцюга збереження доказів (chain of custody).

Успішна реалізація вказаних заходів потребує стратегічного підходу держави до фінансування та матеріально-технічного забезпечення суб'єктів кримінального провадження. Це не може обмежуватися ситуативним виділенням коштів, а має бути системною бюджетною політикою, спрямованою на цифрову трансформацію правосуддя. Передбачення відповідних видатків у державному бюджеті України та їх цільове використання створять реальні умови для формування єдиної технічної

бази, здатної забезпечити належне процесуальне поводження з доказами електронної форми.

Таким чином, забезпечення органів досудового розслідування, прокуратури та судів релевантними технічними й програмними засобами є одним із ключових напрямів удосконалення кримінального процесуального законодавства і практики його реалізації, що дозволить підвищити рівень достовірності, надійності та допустимості доказів досліджуваної категорії у кримінальному провадженні.

Запровадження гешування як механізму підтвердження цілісності доказів електронної форми є давно назрілим. У сфері кримінального процесуального доказування особливої актуальності набуває питання підтвердження автентичності цифрових даних, отриманих у результаті проведення слідчих (розшукових) дій. Ці матеріали, з огляду на їхню електронну природу, є вразливими до несанкціонованих змін, втрат чи підроблень, що в умовах судового розгляду здатне викликати сумніви в їх допустимості або достовірності. Таким чином, забезпечення їх цілісності шляхом використання технічних засобів контролю, зокрема гешування, є не лише бажаним, а об'єктивно необхідним з огляду на вимоги ст. 84 КПК України щодо належного процесуального оформлення джерел доказів. У контексті НСРД це особливо важливо, оскільки результати таких дій, з огляду на їх характер, не мають альтернативних каналів верифікації, окрім технічної. Закріплення геш-значення на момент завершення фіксації матеріалів НСРД забезпечує не лише підтвердження їх цілісності, але й реалізує один з основоположних принципів кримінального провадження – принцип належного процесуального оформлення доказу.

Б. Б. Теплицький (2021) обґрунтовує потребу уточнити ч. 2 ст. 266 КПК України положеннями щодо фіксації геш-суми скопійованих файлів в протоколі НСРД [267, с. 212-213].

Застосування гешування дозволяє гарантувати, що матеріал, отриманий у результаті слідчих (розшукових) дій, не змінювався з моменту його створення або фіксації. Будь-яке навіть мінімальне втручання в структуру файлу призводить до зміни геш-значення, що забезпечує надійний цифровий механізм контролю за

незмінністю доказу. У зв'язку з цим необхідно закріпити на нормативному рівні обов'язок вказувати геш-значення відповідного цифрового об'єкта (наприклад, відеозапису або аудіофрагмента) безпосередньо в протоколі про результати проведення слідчих (розшукових) дій.

У контексті впровадження технічних засобів забезпечення автентичності та цілісності доказів електронної форми важливим є узгодження застосовуваних механізмів із національною системою криптографічного захисту інформації. З цією метою варто було б адаптувати до стандартів Державної служби спеціального зв'язку та захисту інформації України, які визначають перелік дозволених алгоритмів та протоколів у державному секторі.

Окремої уваги потребує процесуальне закріплення використання гешування як обов'язкового інструменту підтвердження цілісності цифрових об'єктів. Доцільно передбачити, що геш-значення повинне фіксуватися безпосередньо у протоколі процесуальної дії та зберігатися поряд з описом файлу чи носія, який долучається до матеріалів кримінального провадження. У такому разі геш виступатиме не лише технічним механізмом перевірки, але й процесуальним реквізитом, що набуває значення невід'ємного атрибута належного оформлення доказу. Це, своєю чергою, забезпечить більшу визначеність при оцінці допустимості таких доказів судом, зменшить ризики сумнівів у їхній автентичності та сприятиме уніфікації практики використання цифрових технологій у кримінальному процесі.

Електронні процесуальні документи є перспективним напрямом розвитку як кримінального процесу України загалом, так і зручного механізму фіксації доказів електронної форми під час кримінального провадження.

Запровадження повністю цифрового протоколу слідчої дії є важливим етапом еволюції кримінального процесу у напрямі цифрової трансформації, що відповідає сучасним викликам, спричиненим інформатизацією суспільства та розвитком технологій. Такий підхід дозволяє забезпечити високий рівень достовірності, оперативності, автоматизації та процесуальної надійності документування інформації, що здобувається у ході слідчих (розшукових) дій. Цифровий протокол

слідчої дії повинен формуватися в режимі реального часу із використанням КЕП усіх процесуальних суб'єктів, залучених до її проведення. Передусім ідеться про підписання протоколу слідчим або прокурором, а також учасниками слідчої дії (свідками, понятими, представниками захисту), які верифікують зміст зафіксованого за допомогою КЕП. За умови неможливості фізичного використання токена КЕП, як у випадку з цивільними особами, може бути застосована ідентифікація через державний сервіс (наприклад, Дія. Підпис із підтвердженням QR-кодом), що відкриває перспективу залучення широкого кола учасників без обмеження в технічних засобах.

Суттєвою складовою цифрового протоколу є обов'язкова відеофіксація слідчих (розшукових) дій. З урахуванням технічних можливостей, доцільно впровадити вимогу щодо гешування відеофайлу після завершення знімання, з наступним включенням отриманого геш-значення до протоколу слідчої дії. Це гарантує можливість підтвердження незмінності результатів відеофіксації та її відповідність задекларованому змісту, зменшуючи ризики фальсифікацій або маніпуляцій.

На рівні практичного впровадження повного цифрового протоколу слід розробити алгоритмізований сценарій дій слідчого, що охоплює: відеофіксацію слідчої дії; створення текстового протоколу із зазначенням геш-ідентифікаторів файлів; підписання всіма учасниками за допомогою КЕП; збереження в централізованому цифровому сховищі із фіксацією електронної позначки часу; автоматичне долучення матеріалів до відповідного провадження в системі e-Case. Уже на цьому етапі існує низка технічних засобів, що дозволяють реалізувати зазначений алгоритм за допомогою наявного ПЗ, однак нормативна база залишається фрагментарною й не уніфікованою.

Серед основних нормативних прогалин варто назвати брак законодавчо визначеного поняття «цифровий протокол слідчої дії», а також обов'язкових вимог до його структури, засобів створення, методів автентифікації та процедур збереження. Необхідним є внесення змін до КПК України та розроблення відомчих

підзаконних нормативних актів, що визначить техніко-правові параметри цифрового протоколу.

Використання КЕП у роботі з доказами електронної форми відкриває нові можливості для підтвердження їхньої автентичності, цілісності та допустимості в межах кримінального провадження. Особливої уваги вимагає не лише підписання процесуальних документів, таких як протоколи, а й окреме підписання самих цифрових файлів, що містять доказову інформацію. Правильне розмежування цих понять має істотне значення для належного правозастосування та правової оцінки відповідних доказів.

Підписання протоколу КЕП є актом, який засвідчує достовірність викладених у ньому обставин, факт фіксації процесуальної дії та підтвердження її здійснення конкретно посадовою особою або учасником слідчої дії. Однак коли йдеться про цифрові файли, які безпосередньо становлять об'єкт доказування (наприклад, електронні листування, відео, файли баз даних, медіафрагменти), КЕП виконує іншу функцію — він гарантує, що конкретний цифровий об'єкт не був змінений з моменту підписання і саме в такому вигляді був вилучений або досліджений. Таким чином, підписання файлів, що вилучаються під час тимчасового доступу до речей і документів, є процесуально значущим актом, який забезпечує підтвердження автентичності та незмінності самих доказових даних, а не лише супровідного протоколу.

Електронна позначка часу, що додається під час підписання КЕП (такого виду, який містить у своєму складі електронну позначку часу), має самостійне юридичне значення. Вона фіксує момент часу, у який було сформовано або підписано файл, і виступає гарантом того, що дані існували у вказаній формі на конкретну дату. У межах кримінального провадження це може мати ключове значення для доведення моменту виявлення, фіксації чи вилучення інформації, особливо коли мова йде про розслідування кіберзлочинів або корупційних злочинів. Використання кваліфікованих засобів електронної позначки часу дозволяє забезпечити незаперечність і юридичну значущість таких доказів під час судового розгляду.

Особливу увагу слід звернути на технологічну єдність механізмів гешування та електронного підпису, які використовують типологічно тотожні криптографічні алгоритми для забезпечення незмінності й ідентифікації даних. Як у процедурі гешування, так і в процедурі підписання КЕП використовуються алгоритми, що перетворюють вхідні дані в унікальний цифровий відбиток (геш), який змінюється за найменшої модифікації оригінального об'єкта. Відповідно, коли цифровий файл підписується КЕП, система формує геш-значення, яке шифрується за допомогою приватного ключа підписанта. Надалі будь-яка особа, яка має відкритий ключ, може перевірити, чи відповідає підпис змісту файлу, й таким чином пересвідчитися у його автентичності та незмінності.

Усі ці механізми разом – підписання цифрових файлів КЕП, додавання електронної позначки часу, гешування – створюють надійну техніко-правову основу для підтвердження достовірності доказів електронної форми. Їх обов'язкове застосування повинно бути нормативно закріплено в КПК України з метою стандартизації процедур та виключення сумнівів щодо допустимості таких.

У площині цифровізації кримінального провадження доцільним видається розроблення єдиного формату електронного протоколу, що забезпечуватиме його машинну зчитуваність та сумісність з електронними інформаційними системами органів кримінальної юстиції (наприклад e-Case). Використання уніфікованого технічного стандарту (наприклад, XML чи іншого сумісного формату) дозволить забезпечити автоматизовану інтеграцію протоколів у цифрове дос'є, спростить їх перевірку, пошук та обробку, а також унеможливить втрату структурованих даних під час обміну між різними органами досудового розслідування, прокуратурою та судом. Запровадження такого стандарту створить передумови для формування єдиного інформаційного простору у сфері кримінальної юстиції та підвищить точність, процесуальну надійність і доказову цінність електронних протоколів.

З огляду на високі ризики втрати або модифікації доказів електронної форми внаслідок технічних збоїв, недбалості або злочинного умислу доцільним є імперативне закріплення в КПК України норми про обов'язковість створення резервних копій доказів електронної форми у визначеному порядку. Така вимога

повинна поширюватися на всі суб'єкти, уповноважені здійснювати слідчі (розшукові) дії або інші процесуальні дії, пов'язані з отриманням чи обробкою доказів електронної форми. Законодавче унормування цього питання створить передумови для належного захисту доказів електронної форми мінімізації процесуальних ризиків та забезпечення більшої впевненості в збереженості зібраних даних на всіх стадіях кримінального провадження.

Доцільно закріпити вимогу щодо виготовлення та зберігання резервних копій належної якості з підтвердженням їх цілісності у визначений ДСТУ спосіб відповідно до пропозицій А. М. Гаркуші [44, с. 43-47].

Упровадження практики використання надійних електронних носіїв інформації, здатних забезпечити довготривале зберігання цифрових даних, є передумовою збереженості доказів досліджуваної категорії. У чинному кримінальному процесуальному законодавстві визначено лише загальні правила щодо речових доказів та документів, однак питання спеціальних вимог до електронних носіїв інформації, що використовуються для зберігання доказів цієї категорії, залишається неврегульованим. Запровадження стандартів використання сертифікованих електронних носіїв інформації має забезпечити належний рівень захисту даних від випадкової втрати, пошкодження чи модифікації.

З технічного погляду особливо важливим є використання носіїв із підвищеною стійкістю до фізичних і кліматичних впливів: температурних коливань, вібрацій, електромагнітних перешкод та вологості. Тут можуть застосовуватися оптичні диски з технологією WORM (write once read many), що забезпечують незмінність даних після їх запису, а також твердотілий накопичувач (SSD) із вбудованими модулями самошифрування. У довгостроковій перспективі доцільно використовувати спеціалізовані архівні носії (наприклад, M-DISC), здатні зберігати інформацію понад 100 років завдяки застосуванню інертних матеріалів.

У контексті забезпечення ефективного функціонування кримінального процесуального механізму з урахуванням доказів електронної форми особливого значення набуває застосування криптографічного шифрування як способу гарантування конфіденційності матеріалів досудового розслідування. У цифрову

епоху, коли передача, обробка та зберігання значної частини матеріалів провадження відбувається у формі електронних даних, гарантії їх захищеності повинні бути реалізовані через технічні та криптографічні засоби.

Теоретико-прикладна модель криптографічного захисту в межах кримінального провадження повинна охоплювати як симетричне, так і асиметричне шифрування інформації, з використанням сертифікованих алгоритмів відповідно до стандартів державної криптографічної політики. Метою шифрування є унеможливлення доступу до змісту електронного файлу (аудіозапису, відеофрагмента, текстового документа) будь-якими сторонніми особами, включно з тими, хто отримав фізичний доступ до носія інформації. У разі належного впровадження шифрування навіть компрометація пристрою або копіювання файлу не призведе до розкриття змісту, оскільки для його розшифрування необхідний приватний ключ або доступ через визначену процедуру.

Серед технічних рішень, які гарантують високий рівень захисту, доцільно виокремити: використання контейнерів із шифруванням даних, реалізацію апаратно-програмних комплексів з автоматичним шифруванням під час запису (full disk encryption), а також застосування КЕП, який поєднує функцію автентифікації та забезпечення незмінності інформації з моменту підписання.

При впровадженні криптографічного захисту треба враховувати специфіку організаційно-процесуальної структури органів досудового розслідування, прокуратури та суду, а також логіку взаємодії між ними. Зокрема, це стосується створення захищених каналів передачі даних, серверної інфраструктури для зберігання зашифрованих копій доказів, а також ПЗ, яке дозволяє відкривати, переглядати, шифрувати й передавати матеріали виключно після автентифікації та авторизації уповноваженого користувача. Особливу увагу слід приділити ризикам зберігання ключів дешифрування, які мають бути надійно ізольовані від основного сховища даних, зберігатися в криптографічних токенах або хмарних середовищах із багаторівневою аутентифікацією.

Крім того, врахування криптографічного шифрування є обов'язковим під час створення та функціонування єдиних державних інформаційно-аналітичних систем

(зокрема, e-Case), у межах яких здійснюється документообіг та обробка доказів електронної форми. Інтеграція криптографічних інструментів у ці системи дозволяє забезпечити виконання вимог конфіденційності, захисту процесуальної інформації, а також формує основу для недопущення втручання у вміст електронного дос'є сторонніми суб'єктами. Таким чином, криптографічне шифрування набуває статусу не лише технічного рішення, а й процесуального гаранта охорони таємниці досудового розслідування, забезпечуючи необхідну правову передбачуваність та захищеність доказів електронної форми в кримінальному процесі.

Шифрування даних у межах кримінального провадження повинно здійснюватися виключно із використанням кваліфікованих засобів криптографічного захисту інформації, які дозволені до застосування в Україні відповідно до державної політики у сфері інформаційної безпеки. Такий підхід гарантує дотримання єдиних стандартів безпеки, унеможливорює використання неперевіраних алгоритмів і забезпечує процесуальну захищеність доказів електронної форми.

Окремо слід наголосити на ризиках, пов'язаних із використанням хмарних сервісів для збереження та обробки цифрових даних. У цьому контексті обов'язковою умовою їх залучення є сертифікація відповідно до вимог українського законодавства, що передбачає підтвердження належного рівня криптографічного захисту, безперервного контролю доступу та дотримання принципів конфіденційності. Лише за умови правової й технічної відповідності такі сервіси можуть застосовуватися у сфері кримінального процесу, не створюючи додаткових загроз для збереження доказів.

Централізоване зберігання та уніфікований облік доказів електронної форми є невід'ємним аспектом ефективної роботи з ними. Окремого значення набуває створення резервних копій та дублювання даних. Використання багаторівневих систем резервного копіювання (наприклад, методологія «3–2–1»: три копії даних, дві на різних носіях, одна — у віддаленому захищеному сховищі) дає змогу мінімізувати ризики втрати доказів унаслідок збоїв або фізичного пошкодження

обладнання. У цій площині важливим є також застосування системи географічно розподілених дата-центрів, які дозволяють підтримувати цілісність і доступність даних навіть у разі техногенних або воєнних загроз. Така система має не лише запобігти втраті або пошкодженню відповідних даних, але й гарантувати дотримання принципів автентичності, цілісності та контрольованості доступу, що є критично важливими з огляду на вимоги допустимості доказів у кримінальному процесі. Пропонована модель передбачає створення національного або регіональних центрів зберігання резервних копій доказів електронної форми інтегрованих із ЄРДР. Доступ до такого сховища здійснюється виключно авторизованими суб'єктами – слідчими, детективами, прокурорами – які визначені як слідчий чи прокурор у відповідному кримінальному провадженні в ЄРДР.

Головним елементом функціонування такого сховища є суворе дотримання принципів безпеки, зокрема – реєстрація всіх транзакцій доступу, запровадження ролей користувачів із чітко визначеними правами, багаторівнева система автентифікації, використання сертифікованих алгоритмів шифрування, а також щоденне створення технічних копій у зашифрованому вигляді. Окрему увагу необхідно приділити реалізації механізмів незворотності та фіксації часу доступу або зміни файлу, що може бути забезпечено завдяки інтеграції технології електронної позначки часу та криптографічного журналювання подій.

З метою довгострокового забезпечення збереженості доказів електронної форми перспективним видається і використання хмарних технологій із застосуванням державних або спеціалізованих серверів, розташованих на території України. За умови сертифікації таких сервісів та застосування криптографічних протоколів передачі даних можливо досягти високого рівня надійності та доступності доказової інформації.

У контексті вдосконалення технічних заходів роботи з доказами електронної форми важливо наголосити, що мова йде не лише про створення резервних копій, але й про уніфікований облік доказів електронної форми. Такий облік повинен передбачати обов'язкове зазначення геш-значення цифрового файлу, його формату, часу збереження та інших атрибутів, які дозволяють ідентифікувати доказ

і підтверджувати його цілісність. Впровадження відповідних технічних механізмів створить можливість простежуваності кожного доказу досліджуваної категорії на всіх етапах кримінального провадження, що забезпечить підвищення рівня процесуальної їх надійності та допустимості.

Слід зазначити, що у відповідь на запитання «Чи існує, на вашу думку, необхідність створення електронної системи для збирання та зберігання доказів електронної форми що міститиме у своєму функціоналі можливості пошуку (наприклад, надсилання електронних запитів) у межах всіх/більшості кримінальних проваджень (для подальшого використання можливих доказів)?» 86% опитаних суб'єктів кримінального провадження вказали на необхідність створення такої системи, 12% не згодні з цією ідеєю, 2% було важко відповісти. І ці результати варто врахувати правоохоронним органам під час планування вдосконалення відомчих електронних інформаційних систем [114, с. 87].

Створення відомчих сховищ цифрових даних, інтегрованих у систему контролю доступу з обов'язковим журналюванням усіх дій відповідно до принципів *chain of custody*, є перспективним напрямом розвитку в досліджуваній сфері. Такі захищені цифрові архіви, інтегровані у відомчу інфраструктуру органів досудового розслідування та прокуратури, повинні функціонувати на базі сертифікованих систем керування даними, підтримувати автоматизований контроль доступу та зберігати всі цифрові сліди, пов'язані з роботою з доказами. Впровадження системи *chain of custody* у цифровій формі дає змогу не лише зберігати інформацію, але й забезпечувати її повну простежуваність на всіх етапах процесуального обігу.

Проблематика обігу доказів електронної форми у кримінальному процесі України виявляється особливо гострою в аспекті ланцюга збереження доказів (*chain of custody*). Одним із ключових бар'єрів для забезпечення належного контролю за цілісністю доказів електронної форми є відсутність централізованої системи обліку електронних носіїв та супровідної технічної інформації щодо них. Наразі в межах різних правоохоронних відомств функціонують ізольовані, внутрішньовідомчі підходи до ведення обліку, що відрізняються за структурою,

наповненням та вимогами до протоколювання. Ця фрагментованість унеможлиблює формування наскрізного аудиту ланцюга зберігання доказів у разі їх передачі між органами досудового розслідування, експертними установами або судами. Крім того, виявляються приклади адміністративного безладдя, коли електронні носії тривалий час перебувають без належного пакування, без ідентифікаційних ознак, без супровідної документації або зі слідами багаторазового відкриття без належної фіксації. Такі явища мають вплив на оцінку судом допустимості відповідних доказів. Розв'язання означеної проблеми вбачається у створенні єдиного сховища доказів електронної форми, що має включати функціонал фіксації контрольних сум, реєстрації кожної операції з доказом, хронології зберігання, переміщення та результатів експертних дій. Такий підхід відповідав би кращим міжнародним практикам і сприяв би підвищенню доказової надійності цифрових слідів у кримінальному провадженні.

Система e-Case є ключовим інструментом цифрової трансформації досудового та судового провадження в Україні. Її запровадження відкрило нові можливості для підвищення прозорості, оперативності, процесуальної дисципліни та загального рівня ефективності кримінального процесу. Основна перевага e-Case полягає в забезпеченні уніфікованого простору для обміну процесуальною інформацією між учасниками кримінального провадження.

Слід зазначити, що окремі правові аспекти введення e-Case – електронної системи управління кримінальними провадженнями щодо корупційних правопорушень, досліджували А. Білецький та М. Цапок (2020) [22, с. 2-30].

Єдиний електронний інформаційний простір органів кримінальної юстиції утворюється при накладенні електронного інформаційного простору на інформаційний простір органів кримінальної юстиції, і отже, володіє ознаками їх обох [104, с. 211]. Електронний інформаційний простір органів кримінальної юстиції включає: а) фізичне середовище – інформаційна інфраструктура, що належить до технологічних й організаційних компонентів інформаційного простору. Вона забезпечує можливість збору, передачі, зберігання, обробки й розповсюдження інформації [84, с. 21]. Сюди відносять інформаційні й

телекомунікаційні системи та мережі зв'язку, індустрії засобів інформатизації, телекомунікації та зв'язку; систем формування і забезпечення збереження інформаційних ресурсів; системи забезпечення доступу до інформаційно-телекомунікаційних систем, мереж зв'язку та інформаційних ресурсів; системи підготовки кадрів, проведення наукових досліджень; алгоритми і програмні засоби, що забезпечують функціонування програмно-апаратних платформ тощо [191]; б) електронне правозастосовне середовище – сукупність програмних засобів, що забезпечують реалізацію електронних кримінальних процесуальних процедур; в) суб'єкти правозастосування – суб'єкти кримінального провадження, що за допомогою інформаційної інфраструктури мають доступ до електронного правозастосовного середовища та забезпечують реалізацію електронного кримінального провадження в межах наданих повноважень. Для ефективного забезпечення завдань електронного кримінального провадження електронне правозастосовне середовище має бути реалізоване у формі єдиного електронного інформаційного поля органів кримінальної юстиції, уніфікований формат якого забезпечить структурування інформаційних потоків та можливість системного автоматизованого електронного аналізу даних, їх контролю [104, с. 211-212].

Забезпечення інтероперабельності розрізнених електронних інформаційних систем органів кримінальної юстиції України є важливою передумовою ефективної роботи з доказами електронної форми. Це пропонується реалізувати за допомогою створення програми-маршрутизатора, яка забезпечить передачу між електронними кримінальними процесуальними правореалізаційними інструментами електронної кримінальної процесуальної інформації, її перекодування (за потреби) відповідно до особливостей тієї чи іншої електронної системи, обробку інформації та її скерування до електронної комірки, журналювання і фіксування руху кримінальних проваджень (справ) [105, с. 67].

Щодо дослідження доказів електронної форми під час судового провадження, інтероперабельність електронних систем дасть змогу сторонам здійснювати цей процес дистанційно у власних особистих віртуальних кабінетах, формувати в електронній системі письмові документи за результатами

дослідження доказів та скеровувати їх до судді. За потреби проблемні питання обговорюватимуться учасниками під час судового розгляду безпосередньо або дистанційно. Можливі два формати дистанційної взаємодії: 1) відеоконференцзв'язок; 2) текстовий (письмовий) електронний діалог. Останній передбачає використання письмової мови в інтерактивному режимі з наступним автоматичним формуванням електронного процесуального документа визначеного формату (шаблону) згідно з внесеними учасниками провадження письмовим текстом та відмітками. Також, на нашу думку, необхідним є запровадження двох режимів текстового електронного діалогу: online для процесуальних процедур, що потребують негайного вирішення чи створюють загрозу розголошення матеріалів кримінального провадження в контексті впливу на свідків тощо; та offline з відстрочкою часу для надання відповіді (кілька годин/днів на внесення даних за існуючими даними чи поставленими питаннями, завданнями). Таким чином можна суттєво скоротити тривалість судових засідань, вирішуючи низку питань дистанційно [105, с. 69].

Отже, ефективна робота з доказами електронної форми потребує належного технічного та ПЗ органів досудового розслідування, прокуратури і судів. Визначальними є уніфіковані стандарти обладнання й програмних засобів, сертифікація їх використання та централізована система технічного контролю. Ключовими інструментами підтвердження автентичності й цілісності доказів є гешування, КЕП та електронна позначка часу, що доцільно відображати у протоколах як обов'язкові реквізити підтвердження цілісності цифрових даних. Додаткові гарантії створюють системи автоматичного журналювання доступу та впровадження chain of custody у цифровій формі. Важливим напрямом є створення резервних копій і захищених сховищ, інтегрованих з електронними інформаційними системами органів кримінальної юстиції, із жорстким контролем доступу, багаторівневим шифруванням і географічним дублюванням даних.

5.4. Концепція вдосконалення інституту доказів електронної форми у кримінальному процесі України

Як результат проведеної в цьому дисертаційному дослідженні системної наукової розвідки нами сформовано концептуальне бачення комплексного вдосконалення роботи з доказами електронної форми у кримінальному процесі України, що базується на системному поєднанні нормативних, організаційних, інфраструктурних, техніко-криміналістичних, освітніх та науково-аналітичних заходів.

1. Загальні положення Концепції.

Стратегічною метою цієї Концепції визначено створення ефективного, цілісного та технологічно узгодженого механізму процесуального обігу доказів електронної форми, здатного забезпечити достовірність, автентичність і цілісність даних під час кримінального провадження, відповідно до міжнародних стандартів та найкращих світових практик.

Ця стратегія розроблена відповідно до положень та узгоджується з цілями С.2 та С.3 розділів 5 та 6 Стратегії кібербезпеки України, схваленої рішенням Ради національної безпеки і оборони України від 14 травня 2021 року та уведеною в дію Указом Президента України від 26 серпня 2021 р. № 447/2021; пунктами 10, 16, 26 Плану реалізації Стратегії кібербезпеки України, схваленого рішенням Ради національної безпеки і оборони України від 30 грудня 2021 р. та уведеного в дію Указом Президента України від 1 лютого 2022 р. № 37/2022; пунктами 5.1-5.9 Розділу II Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки, схваленого Указом Президента України від 11 травня 2023 р. № 273/2023; пунктами 2.7, 3.1.1, 3.1.2, 3.2, 3.3, 3.3.1-3.3.4, 4.5, 4.6 Стратегії розвитку прокуратури на 2025-2028 роки, затвердженої наказом Генерального прокурора № 322 від 8 жовтня 2025 р.

Обсяг правовідносин, що охоплюються Концепцією включає процесуальні правовідносини на всіх стадіях кримінального провадження.

Адресатами цієї Концепції є законотворці, очільники органів досудового розслідування, прокуратури, судової системи, експертних установ, центральні органи виконавчої влади, здатні формувати та реалізувати державну політику в сфері кримінальної юстиції.

2. Нормативний напрям передбачає внесення системних змін до КПК України (див. Додаток І), що визначатимуть правовий статус доказів електронної форми, механізми підтвердження їх цілісності та критерії допустимості, процедури їх здобуття а також імплементації положень Конвенції про кіберзлочинність, ДСТУ ISO/IEC 27037:2017 та Протоколу Берклі, що включає:

- внесення змін до КПК України: доповнити положеннями, що визначатимуть правовий статус таких доказів, критерії їх допустимості, а також процедури їх збирання, перевірки, оцінки й подання у суді;

- нормативно закріпити необхідність створення СОП;

- внесення змін до Законів України щодо зберігання інформації ітд, вимог до представників органів досудового розслідування, прокурорів та суддів, їх спеціалізації;

- прийняття міжвідомчого підзаконного НПА щодо взаємодії органів досудового розслідування та органів прокуратури з НКП 24/7;

- прийняття суб'єктами кримінального провадження відомчих актів щодо організації роботи з доказами досліджуваної категорії;

2.1. Оновлення термінологічної бази КПК України.

Законопроект вводить до КПК України низку нових дефініцій, що мають бути інкорпоровані в Концепцію як базові: дані про рух інформації; дані, які зберігаються; електронний носій інформації; комп'ютерні дані; комп'ютерна система; кіберпростір; матеріальний носій інформації; цілісність інформації та цілісність комп'ютерних даних.

У Концепції це дозволяє чітко розмежувати правовий режим трьох категорій джерел доказів:

- матеріальні носії інформації;

- електронні носії інформації та комп'ютерні системи (диск, флеш-накопичувач, телефон);
- віртуальні середовища (хмарні сервіси, акаунти, мережеві середовища).

2.2. Автентичність і цілісність доказів електронної форми.

Концепція деталізує:

- обов'язковість підтвердження цілісності доказів електронної форми за допомогою технічних засобів: гешування, контрольні суми, журнали доступу, метадані, цифрові ідентифікатори;
- необхідність ведення ланцюга збереження доказів (chain of custody), включаючи фіксацію всіх дій з доказом, створення резервних копій, застосування технічних засобів контролю доступу;
- можливість використання розподілених реєстрів як факультативного механізму фіксації незмінності.

2.3. Нормативне врегулювання процесів збирання та здобуття доказів електронної форми.

Концепція деталізує нове нормативне розмежування:

- збирання — фізичне вилучення EIC, KC, MTCЗ;
- здобуття — копіювання / створення образу ЕНІ.

Встановлюється принцип «копія — перед вилученням», коли вилучення обладнання є крайньою мірою.

2.4. Регулювання кіберпроцедур і OSINT.

У Концепцію інтегруються нові регуляції: огляд віртуального середовища; пошук відомостей у відкритих джерелах (OSINT) з фіксацією логіки дій, переходів, технічних параметрів та метаданих; уніфікація та стандартизація використання інструментів OSINT.

2.5. Тимчасовий доступ, термінове збереження й аналіз даних про рух інформації.

Концепція доповнюється: моделлю термінового збереження комп'ютерних даних на 90 днів (з можливістю продовження ще на 90 днів); порядком тимчасового

розкриття даних про рух інформації; процедурою роботи з провайдерами електронних комунікацій.

2.6. Захист приватності та обмеження втручання.

За допомогою запропонованих у законопроекті нових положень ст. 236 КПК України буде забезпечено механізми мінімізації втручання у приватність; розмежування доступу до листування та доступу до комп'ютерних даних; необхідність окремої ухвали слідчого судді для доступу до приватної комунікації.

3. Організаційний напрям.

3.1. Ефективна взаємодія між суб'єктами кримінального провадження.

- стандартизація практики правозастосування шляхом розробки СОП щодо роботи з доказами електронної форми, який має визначати порядок ідентифікації, фіксації, збирання, здобуття, передачі та зберігання таких доказів, для кожного з суб'єктів кримінального провадження (органи досудового розслідування, прокуратура, суди тощо – окремі СОП), що не є НПА та врегульовують відповідну роботу на відомчому рівні. Хоча окремі методичні рекомендації та внутрішньовідомчі інструкції містять важливі положення, відсутність єдиного загальнообов'язкового стандарту для всіх органів досудового розслідування унеможливорює формування послідовної практики правозастосування;

- розширення практики ефективної взаємодії між суб'єктами кримінального провадження в межах міжвідомчої співпраці, що є необхідною умовою забезпечення належної роботи з доказами електронної форми. Вона передбачає узгодженість у процесуальних діях, обмін знаннями та ресурсами, залучення спеціалістів і створення сталих каналів комунікації між слідчими, прокурорами, спеціалістами, експертами та судом;

- проведення суб'єктами кримінального провадження аналітичної роботи щодо оцінки практики правозастосування у сфері роботи з доказами електронної форми;

3.2. Системні рішення щодо посилення кадрового потенціалу. Кадрова спроможність органів досудового розслідування, прокуратури, суду та експертних установ. Відсутність чітко визначених кваліфікаційних вимог до осіб, які

здійснюють первинний контакт з електронними носіями інформації, дефіцит міждисциплінарних знань і навичок, брак кваліфікованих спеціалістів, а також нерівномірність підготовки між різними підрозділами створюють ризики втрати доказів або визнання їх недопустимими. Вирішення цього завдання потребує:

- уніфікації підходів до підготовки юридичних та правоохоронних кадрів на рівні вищих навчальних закладів юридичного (спеціальність «Право» та «Правознавство») та правоохоронного (спеціальність «Правоохоронна діяльність») профілів;

- запровадження спеціалізації слідчих, дізнавачів та прокурорів в частині кримінальних проваджень щодо кіберзлочинів а також проваджень, що містять значну кількість доказів електронної форми;

- створення у складі органів досудового розслідування криміналістичних ІТ-лабораторій, що структурно відокремлені від органів досудового розслідування та організаційно не підпорядковані його керівнику;

- впровадження ефективного професійного навчання (підвищення кваліфікації) суб'єктів кримінального провадження) в.тому числі впровадження програм міжвідомчого навчання;

3.3. Створення сталого каналу комунікації з провайдерами телекомунікації та налагодження шляхів ефективної взаємодії, створення спільних міжвідомчих робочих груп

4. Інфраструктурний напрям.

4. Налагодження електронних кримінальних процесуальних процедур між суб'єктами кримінального провадження в частині обміну доказами електронної форми під час кримінального провадження а також реалізації електронних кримінальних процесуальних процедур.

4.1. Створення безпечного механізму електронного обміну ними між суб'єктами кримінального провадження - інтегрованої системи управління доказами, що має забезпечити централізований облік, автоматизований контроль доступу, фіксацію дій уповноважених осіб і формування електронного дос'є, синхронізованого з ЄРДР та e-Case.

Зберігання доказів електронної форми та контроль доступу до них потребує нормативного врегулювання та технологічного забезпечення. Необхідним є створення відомчих віртуальних сховищ (цифрових архівів) для зберігання резервних копій доказів електронної форми.

4.2. Створення цифрової інфраструктури для забезпечення комунікації органів досудового розслідування та прокуратури з провайдерами телекомунікації та налагодження цифрової форми реалізації процесу виконання ухвал про тимчасовий доступ до речей і документів щодо даних операторів телекомунікації.

5. Техніко-криміналістичний напрям.

5.1. Матеріально-технічне забезпечення органів досудового розслідування, прокуратури та суду на належному рівні. Відсутність спеціалізованого обладнання й ПЗ, а також нерівномірний рівень оснащення різних відомств істотно ускладнює ідентифікацію, вилучення та дослідження доказів електронної форми. Тому необхідне забезпечення органів досудового розслідування, органів прокуратури та суду релевантними технічними та програмними засобами;

5.2. Стандартизація форматів зберігання доказів електронної форми, методів ідентифікації та застосовуваних суб'єктами кримінального провадження інструментів цифрової криміналістики. Пропонується впровадження уніфікації та внутрішньої сертифікації програмних і апаратних засобів, що застосовуються для обробки доказів електронної форми.

Деградація ЕНІ на яких зберігаються докази досліджуваної форми, відсутність централізованих сховищ і недосконалість механізмів розмежування доступу створюють ризики втрати або спотворення доказів. Необхідним є:

- запровадження гешування як механізму підтвердження цілісності доказів електронної форми;
- врегулювання практики використання електронних процесуальних документів;
- запровадження практики резервного копіювання доказів досліджуваної категорії,

- використання надійних електронних носіїв інформації під час фіксації доказів електронної форми, здатних забезпечити довготривале зберігання даних;
- криптографічне шифрування цифрових даних, що є доказами.

6. Освітній напрям.

6.1. Впровадження в освітні програми вищих навчальних закладів юридичного (спеціальність «Право» та «Правознавство») та правоохоронного (спеціальність «Правоохоронна діяльність») профілів компетентностей щодо роботи з доказами електронної форми, інформаційної безпеки, цифрової комунікації;

6.2. Підвищення кваліфікації суб'єктів кримінального провадження, зокрема:

- обов'язкове професійне навчання слідчих, дізнавачів та прокурорів з цифрової криміналістики; вивчення механізмів гешування, аналізу метаданих, ідентифікації електронних підписів та їх первинної оцінки, роботи з системами електронного документообігу;
- постійне та послідовне підвищення рівня цифрової компетентності слідчих, дізнавачів, прокурорів, суддів;
- формування для слідчих, дізнавачів, прокурорів, суддів вимог щодо обов'язкових міждисциплінарних цифрових компетентностей.

7. Науково-аналітичний напрям.

7.1. Розширення та інституційна підтримку наукових досліджень за відповідною тематикою, що полягає у формуванні Національною академією правових наук України окремих наукових напрямів щодо цифрової складової кримінального процесу України (за результатами системного опрацювання аналітичних матеріалів суб'єктів правозастосування);

7.2. Здійснення науково-дослідними установами системних наукових досліджень доказів електронної форми під час кримінального провадження, спрямовані на розв'язання конкретних практичних завдань та вдосконалення практики правозастосування;

7.3. Здійснення наукових досліджень закордонного досвіду роботи з доказами електронної форми під час кримінального провадження в частині їх технічних аспектів;

7.4. Забезпечення постійного моніторингу суб'єктами кримінального провадження практики застосування доказів електронної форми під час кримінального провадження та публікації щорічних оглядів стану використання таких доказів у кримінальному провадженні. Посилення координуючої ролі органів прокуратури в цьому напрямі та визначення провідної ролі науково-методичної ради при Офісі Генерального прокурора. Вказане передбачає:

- здійснення систематичного аналізу судових рішень з відповідним напрямом, формування та публікація аналітичних узагальнень;
- постійну (щорічну) актуалізацію СОП;
- створення аналітичної бази судових рішень;
- постійний аудит інфраструктури та процедур;
- щорічне державне звітування про стан реалізації цієї Концепції.

8. Очікувані результати та строки реалізації

Очікувані результати від заходів цієї Концепції полягають у формування серед суб'єктів кримінальної юстиції України сталої практики роботи з доказами електронної форми під час кримінального провадження, заснованої на наукових підходах.

8.1. Нормативно-правова трансформація системи кримінального провадження.

8.1.1. Формування цілісного законодавчого масиву, сумісного з міжнародними стандартами

У результаті системного оновлення КПК України та суміжних НПА відбудеться перехід від фрагментарного регулювання до структурно збалансованої нормативної моделі, що комплексно охоплює всі аспекти роботи з доказами електронної форми. Введення дефініцій (комп'ютерні дані, дані про рух інформації, електронний носій інформації, цілісність комп'ютерних даних, ланцюг збереження доказів тощо) забезпечить однозначність правового тлумачення, що усуває прогалини й суперечності, котрі тривалий час унеможлилювали стабільність правозастосовної діяльності. Оновлена нормативна основа стане структурно сумісною з Конвенцією про кіберзлочинність, рекомендаціями Ради

Європи та технічними стандартами ISO/IEC 27037:2017, що забезпечить інтеграцію українського кримінального процесу у глобальний цифровий правовий простір.

8.1.2. Створення процесуально повноцінної моделі використання доказів електронної форми.

Імплементация нових процесуальних інститутів – збирання та здобуття доказів електронної форми, термінове збереження даних, ланцюг збереження доказів, огляд віртуального середовища, OSINT, перехоплення даних про рух інформації – забезпечить формування єдиної логічної системи, у якій кожна дія з цифровими даними має чіткий процесуальний статус, форму, технічні вимоги та юридичні наслідки. Це підвищить доказову спроможність інформації у цифровій формі та посилить мотивованість судових рішень.

8.2. Інституційне та організаційне зміцнення системи кримінальної юстиції.

8.2.1. Встановлення уніфікованих стандартів діяльності суб'єктів кримінального провадження.

Розроблення та впровадження СОП усіма органами досудового розслідування, прокуратури, судами призведе до утворення уніфікованої системи відомчих стандартів, що забезпечують: 1) передбачуваність процесуальних дій; 2) однаковість техніко-криміналістичних підходів; 3) виключення суб'єктивного «відомчого розуміння» вимог закону. Стандартизація сприятиме формуванню єдиної методології обігу доказів електронної форми в кримінальному процесі, що унеможливить втрату інформації через недотримання технологічних процедур.

8.2.2. Поглиблення міжвідомчої взаємодії.

Завдяки створенню сталих комунікаційних механізмів між органами досудового розслідування, прокуратури, суду, операторами телекомунікацій та НКП 24/7 виникне нова модель координаційної взаємодії, у якій: 1) цифрові сліди не втрачатимуться через затримки в комунікації; 2) вимоги до надання даних провайдерами стануть прогнозованими та врегульованими; 3) усі суб'єкти працюватимуть в межах єдиної цифрової інфраструктури. Це перетворить фрагментовану систему на інтероперабельну платформу, сумісну з європейською моделлю обігу доказів електронної форми.

8.2.3. Підвищення кадрової спроможності.

Інституційне впровадження нових кваліфікаційних вимог, спеціалізацій та програм підготовки з правової інформатики та цифрової криміналістики зумовить структурне перезавантаження кадрового потенціалу органів кримінальної юстиції. Очікуваним є утворення: 1) професійних груп цифрових слідчих (digital investigators); 2) мережі технічно підготовлених прокурорів; 3) експертних підрозділів з компетенцією роботи з криміналістичними (побітовими) копіями (образами носіїв), метаданими, журналами доступу тощо; 4) суддів з цифровою процесуальною компетентністю. Завдяки цьому підвищиться

8.3. Розбудова цифрової інфраструктури кримінального провадження.

8.3.1. Функціонування інформаційної системи зберігання доказів електронної форми.

Створення державної системи зберігання цифрових доказів забезпечить: 1) автоматизований контроль доступу до доказів електронної форми у режимі реального часу; 2) фіксацію метаданих і цифрових ідентифікаторів, що суттєво знизить ризик спотворення, підробки чи маніпуляції; 3) створення електронного зв'язку між доказами електронної форми та відомостями ЄРДР та e-Case, що підвищить інтероперабельність електронних інформаційних систем органів кримінальної юстиції; 4) резервне копіювання доказів електронної форми, що унеможливило втрату; 5) фіксація chain of custody. Це засвідчить перехід від застарілої практики зберігання електронних носіїв інформації у сейфах до інституційної цифрової екосистеми, що гарантує збережуваність та незмінність цифрових даних.

8.3.2. Формування віртуальних архівів органів правопорядку.

Реалізація вимог до віртуальних архівів (Офіс Генерального прокурора, Міністерство юстиції України, Міністерство цифрової трансформації) становитиме перший в Україні приклад створення загальнодержавної інтероперабельної цифрової інфраструктури кримінальної юстиції, здатної забезпечити довгострокове зберігання електронних доказів із використанням криптографічних механізмів захисту.

8.3.3. Електронний обмін електронними даними, що є доказами у кримінальному провадженні.

Впровадження стандартизованих електронних каналів обміну цифровими даними в кримінальному провадженні (включно з можливістю автоматичного виконання ухвал про тимчасовий доступ) спричинить: 1) різке скорочення часу передачі доказів електронної форми; 2) виключення ризиків втрати доказів при фізичній передачі; 3) гарантоване дотримання контролю доступу та фіксація chain of custody.

8.4. Удосконалення техніко-криміналістичних механізмів.

8.4.1. Уніфікація технічних процедур і цифрових стандартів.

Після реалізації заходів пропонованої Концепції усі суб'єкти кримінального провадження працюватимуть з доказами електронної форми за єдиними технічними стандартами — від моменту ідентифікації цифрового джерела до його дослідження експертною установою. Єдиний стандарт гешування, вимоги до журналів доступу, протоколів копіювання, процедур OSINT та огляду кіберпростору забезпечать: 1) відтворюваність процесуальних процедур; 2) технічну сумісність дій між різними органами досудового розслідування; 3) істотне зменшення кількості технічних помилок, що потенційно призводять до визнання доказів недопустимими.

8.4.2. Матеріальне забезпечення, здатне забезпечити реалізацію сучасних практик цифрової криміналістики.

Впровадження сучасних інструментів (форензик-комплексів, програм для створення бітових образів, засобів фіксації мережевого трафіку, криптографічних модулів) дозволить: 1) максимально точно відтворювати технічний контекст вилучених даних; 2) проводити технічні дослідження без ризику пошкодження інформації; 3) стандартизувати аналіз цифрових слідів. У довгостроковій перспективі це призведе до підвищення доказової цінності цифрових даних, що сьогодні нерідко оспорується у судах через технічні недоліки їх фіксації.

8.5. Підвищення ефективності освітнього середовища та розвитку компетентностей суб'єктів кримінального провадження

8.5.1. Інтеграція цифрової криміналістики в юридичну освіту

Результатом стане перехід від факультативного вивчення доказів електронної форми до повноцінної інтеграції цифрових компетентностей у зміст юридичної освіти, включно з: 1) роботою з комп'ютерними даними та їх метаданими; 2) техніками OSINT-добування; 3) основами криптографічного захисту; 4) аналізом цифрового ланцюга збереження. Це закладе фундамент для підготовки нового покоління юристів, здатних працювати у цифровому кримінальному процесі.

8.5.2. Підвищення кваліфікації кадрів.

Сформується інституційна система підвищення кваліфікації в частині цифрової підготовки, що забезпечить: 1) постійне оновлення компетентностей; 2) адаптацію до нових технологій; 3) зменшення інституційного опору цифровим реформам.

8.6. Розвиток науково-аналітичного забезпечення кримінального процесу.

8.6.1. Створення наукової школи цифрової доказовості.

Завдяки формуванню національного наукового напрямку з цифрової складової кримінального провадження в частині доказів електронної форми, українська правова думка отримає: 1) нову предметну область теоретичних досліджень; 2) академічне підґрунтя для техніко-правових новацій; 3) інституційну платформу для розроблення СОП.

6.2. Регулярний аудит судової практики і технічної інфраструктури.

Системний моніторинг дозволить: 1) виявляти типові помилки та прогалини практики роботи з доказами електронної форми; 2) формувати щорічні аналітичні звіти; 3) запобігати звуженню змісту законодавчих інновацій через практичну інерцію.

У результаті практика, наука та законодавство функціонуватимуть синхронно та взаємодіятимуть у режимі взаємного зворотного зв'язку.

8.7. Загальний системний ефект впровадження заходів Концепції.

8.7.1. Підвищення якості правосуддя.

Завдяки комплексній модернізації інституту доказів електронної форми у кримінальному процесі України забезпечується: 1) підвищення точності

встановлення фактів під час судового розгляду; 2) зменшення ризику визнання доказів електронної форми недопустимими; 3) збільшення передбачуваності судових рішень, їх обґрунтованості.

8.7.2. Ефективний захист фундаментальних прав людини.

Система мінімізації втручання у приватність, окремі гарантії доступу до електронних комунікацій, прозорі механізми журналювання доступу до цифрової інфраструктури створюють нову якість правових гарантій, що поєднує ефективність кримінального провадження та дотримання прав людини.

8.7.3. Зміцнення довіри суспільства.

За результатами реалізації заходів пропонованої Концепції суспільство отримає: 1) більше прозорості; 2) менше можливостей для маніпуляцій з електронними даними; 3) науково обґрунтований процес доказування під час кримінального провадження, який відповідає сучасним технологічним викликам.

Початок реалізації заходів цієї Концепції доцільно визначати в межах Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки, схваленого Указом Президента України від 11 травня 2023 р. № 273/2023.

Кінцеві строки реалізації пропонованої нами Концепції доцільно визначити в межах 10 років від початку її реалізації за умови ефективної нормативної регламентації (ухваленням ключових законодавчих змін), системної підтримки всіма суб'єктами кримінального провадження та адекватного фінансування.

ВИСНОВКИ

У дисертації на основі комплексного аналізу доктринальних положень вітчизняних і зарубіжних учених у галузі права та дотичних спеціальностей, актів національного законодавства, міжнародно-правових документів та сталої кримінальної процесуальної практики правозастосування вирішено важливу наукову проблему, що полягає у науковому обґрунтуванні концептуальних засад інституту доказів електронної форми у кримінальному процесі України, визначенні їх процесуально-правової природи, особливостей джерел походження, порядку ідентифікації, збирання, здобуття, процесуальної фіксації, зберігання і використання, а також у розробленні теоретико-методологічних та організаційно-практичних підходів до вдосконалення кримінального процесуального регулювання діяльності суб'єктів кримінального провадження щодо роботи з такими доказами в умовах глобальної цифровізації, а саме:

1. Категорія доказів у кримінальному процесі України є результатом тривалої еволюції наукової думки та має багатовимірну правову природу. Інтегративний підхід до розуміння доказів у кримінальному процесі України ґрунтується на узгодженні інформаційного, логічного та формально-процесуального вимірів доказування і відображає сучасний стан доктринального осмислення цієї категорії. У такому підході доказ сприймається не як абстрактна інформація чи ізольований факт, а як єдність фактичних даних, їх джерел і процесуальної форми, що набувають доказового значення внаслідок реалізації уповноваженими суб'єктами кримінального провадження передбачених законом процесуальних повноважень. Властивості доказів (належність, допустимість, достовірність і достатність) виступають загальними критеріями їх оцінки незалежно від способу фіксації чи виду матеріального носія. За такого розуміння електронна форма постає не як підстава для виокремлення самостійного виду доказів, а як характеристика способу існування й подання фактичних даних у межах усіх визначених в ст. 84 КПК України процесуальних джерел доказів, специфіка якої проявляється насамперед через

розширення можливостей перевірки автентичності та цілісності відомостей як складової забезпечення їх допустимості та достовірності.

2. Електронна складова кримінального процесу України складається з п'яти елементів: електронне кримінальне провадження; оцифрування матеріалів кримінальних проваджень та їх резервне зберігання; докази електронної форми; електронні інструменти доказування; електронні інструменти реалізації повноважень суб'єктів правозастосування. Розуміння правової природи вказаних елементів та їх неототожнення є передумовою коректного правозастосування.

«Цифровий доказ» відповідає змісту доказу, «електронний доказ» – технічному способу його реалізації, а «доказ електронної форми» – процесуальній формі подання. Нормативна уніфікація поняттєвого апарату досліджуваної сфери є необхідною умовою побудови ефективної системи роботи з доказами електронної форми в кримінальному процесі України.

3. Передумови становлення інституту доказів електронної форми в кримінальному процесі України зумовлені як технологічним розвитком, що збільшив обсяг електронних даних у кримінальних провадженнях, так і внутрішньою потребою кримінальної процесуальної науки висвітлити власне бачення нової цифрової реальності. Становлення відповідного інституту характеризується конкуренцією доктринальних підходів (від ототожнення з документами чи речовими доказами до пропозицій їх виокремлення як самостійного процесуального джерела доказів) та значною термінологічною варіативністю. Потреба переосмислення доказів електронної форми у кримінальному процесі України як самостійного інституту вимагає уніфікованого, послідовного, комплексного та технологічно орієнтованого доктринального та нормативного супроводу, заснованого на концептуальному баченні поетапного формування спеціальних процесуальних режимів, уникаючи різких нормативних змін, здатних дестабілізувати систему доказування.

4. Процесуальна природа доказів електронної форми у кримінальному процесі полягає у можливості їх потенційної належності до всіх процесуальних джерел доказів, визначених ст. 84 КПК України. Факт належності доказу досліджуваної

категорії до певного процесуального джерела визначає процесуальний порядок поводження з ними під час кримінального провадження та, як наслідок, критерії оцінки його допустимості. Електронна форма фіксації показань (шляхом застосування відеозапису) є допустимим у контексті ст. 225, ч. 11 ст. 615 КПК України способом здобуття релевантного для суду доказу, що не змінює їх особистісної сутності, але висуває додаткові вимоги до автентифікації допитуваної особи, збереження результатів фіксації та перевірки їх цілісності. Документами докази досліджуваної категорії визначаються через призму п. 1 та п. 3 ч. 2 ст. 99 КПК України, а також електронних документів, підписаних КЕП (у розумінні профільного закону). Речові докази репрезентовані фізичними об'єктами – електронними носіями інформації або технічними пристроями, щодо яких доказове значення має саме зафіксована на них інформація, тож їх визнання речовим доказом обумовлене потребою встановлення належного правового режиму при їх вилученні – арештом майна. При цьому слід чітко розмежовувати носій інформації, на якому за допомогою технічних засобів зафіксовано процесуальні дії – як документ (п. 3 ч. 2 ст. 99 КПК України), та матеріальний об'єкт, що охороняється у статусі майна, – як речовий доказ. Висновок експерта дедалі частіше набуває електронної форми й потребує підписання кваліфікованим електронним підписом, що вимагає забезпечення його належного процесуального оформлення, підтвердження автентичності та відтворюваності.

Технічна природа доказів електронної форми визначається сукупністю характеристик інформаційного середовища, у якому вони створюються та зберігаються, а також властивостями електронних носіїв інформації, що досліджуються під час кримінального провадження. Доказ електронної форми функціонує як чотирирівнева структура: контент, метадані, системна оболонка та електронний носій інформації, що має матеріальне вираження. Запропонована у дослідженні класифікація електронних носіїв інформації (за доступністю, середовищем зберігання, типом пам'яті, ступенем інтеграції з ІС) безпосередньо впливає на вибір процесуальних рішень: підходи до виявлення й вилучення, обґрунтування арешту майна, пріоритизацію фіксації нестабільних даних тощо.

Важливими для доказування під час кримінального провадження є технічні аспекти доказів досліджуваної категорії: метадані; розмежування логічного копіювання (окремих файлів) і побітового (криміналістичного) копіювання (створення образу електронного носія інформації); гешування; електронний підпис та електронна позначка часу. Гешування забезпечує відтворювану ідентифікацію цифрового об'єкта та виявлення будь-яких змін, слугуючи технічною основою для підтвердження цілісності та незмінності комп'ютерних даних. Відповідні технічні характеристики доказів електронної форми, що здатні підтвердити автентичність та цілісність цифрових даних, в сукупності з належними кримінальними процесуальними процедурами становлять дуалістичну основу процесуальної допустимості доказів електронної форми у кримінальному провадженні.

5. Комплекс алгоритмів пошуку та фіксації доказів електронної форми об'єднаний за трьома функціонально-структурними категоріями і розглядається як три стратегії фіксації доказів електронної форми у кримінальному процесі України: 1) фізичне вилучення електронних носіїв інформації або комп'ютерних систем; 2) огляд та копіювання комп'ютерних даних; 3) огляд та фіксація інформації з відкритих джерел. Пропонована модель визначає копіювання комп'ютерних даних, здійснене з дотриманням вимог ч. 4 ст. 99 КПК України (за участю спеціаліста) та норм ДСТУ ISO/IEC 27037:2017, пріоритетною та технологічно доцільною альтернативою фізичному вилученню технічних пристроїв. Фіксація інформації з відкритих джерел розглядається як самостійний напрям здобуття доказів електронної форми, що на практиці реалізується через призму огляду (ст. 237) або слідчого експерименту (ст. 240), ґрунтується на використанні методології Протоколу Берклі, програмних засобів OSINT, та, в окремих випадках, застосуванні механізмів Конвенції про кіберзлочинність та процедур міжнародної правової допомоги під час кримінального провадження.

6. Підтвердження цілісності та автентичності доказів електронної форми в кримінальному процесі ґрунтується на поєднанні техніко-криміналістичних інструментів ідентифікації комп'ютерних даних і процесуальних вимог послідовної фіксації й перевірки таких ідентифікаторів, контролю доступу та забезпеченні

безпеки доказів досліджуваної категорії, що вибудовують багаторівневу систему. Ідентифікація комп'ютерних даних під час кримінального провадження розглядається через призму абз. 3 п. 3 ч. 3 ст. 104 КПК України та п. 5.4.2 ДСТУ ISO/IEC 27037:2017 як процесу, покликаного забезпечити встановлення тотожності комп'ютерних даних на всіх стадіях кримінального провадження, підтвердження їх цілісності та автентичності. Практично значущі механізми, що застосовуються для досягнення цієї мети, доцільно систематизувати за ступенем зростання рівня надійності: упакування та маркування електронних носіїв інформації; фіксація загальних та унікальних апаратних ідентифікаторів; опис структури і змісту комп'ютерних даних та їх метаданих; ґешування комп'ютерних даних і послідовної фіксації контрольних сум комп'ютерних даних в процесуальних документах; використання КЕП та електронної позначки часу. Системне дослідження концепції chain of custody, її організаційно-технічних моделей засвідчило необхідність її подальших системних досліджень та перспективу інституціоналізації у національній практиці.

7. Ефективність оперування доказами електронної форми у кримінальному процесі України визначається організаційною спроможністю інституцій кримінальної юстиції. Організаційну готовність суб'єктів кримінального провадження до роботи з доказами електронної форми доцільно розглядати через три взаємопов'язані компоненти: 1) матеріально-технічний – охоплює забезпечення органів досудового розслідування, прокуратури та суду цифровими криміналістичними інструментами та інфраструктурою, сумісною з ДСТУ ISO/IEC 27037:2017; 2) кадровий – пов'язаний зі створенням в структурі органів досудового розслідування криміналістичних ІТ-лабораторій для роботи з доказами електронної форми, міждисциплінарною компетентністю слідчих, детективів, прокурорів, спеціалістів, експертів і суддів, їх профільною спеціалізацією та системним підвищенням кваліфікації; 3) нормативний – окреслює необхідність запровадження єдиних стандартів роботи з доказами досліджуваної категорії для всіх суб'єктів кримінального провадження, забезпечення надійного зберігання таких доказів та контролю доступу до них.

8. Роль слідчого у роботі з доказами електронної форми є системоутворювальною: від його фаховості, своєчасних процесуальних рішень і технічно коректної взаємодії з цифровим середовищем залежить доказова спроможність отриманих даних. Ефективність такої діяльності передбачає поєднання правових навичок із базовою цифровою грамотністю: розуміння природи комп'ютерних даних і метаданих, механізмів логічного захисту та гешування, відмінностей між логічним і побітовим копіюванням, а також практичне володіння інструментами OSINT для оперативного виявлення релевантних слідів. Протоколи слідчих (розшукових) дій мають відтворювати технічний контекст одержання даних, характеристики електронних носіїв інформації і комп'ютерних систем, спосіб та параметри ідентифікації (геш значення), а також фіксувати будь-які впливи на цифрове середовище. Процесуально значущим є виважений вибір слідчого між фізичним вилученням носія та копіюванням інформації, що повинен спиратися на сукупність процесуальних і технічних умов.

9. Прокурор у кримінальному провадженні виступає ключовим суб'єктом забезпечення належного обігу доказів електронної форми, поєднуючи координацію дій слідчого, оперативних підрозділів, спеціаліста й експерта, контроль за дотриманням критеріїв належності, допустимості й достовірності. Його повноваження охоплюють (але не обмежуються): вибір способу одержання відомостей (копіювання інформації чи вилучення носія інформації), фіксацію ідентифікаційних параметрів комп'ютерних даних (зокрема геш-значень) у протоколах, перевірку автентичності електронних документів і електронних підписів, організацію відкриття матеріалів досудового розслідування стороні захисту відповідно до ст. 290 КПК України, а також використання механізмів міжнародної взаємодії. На стадії судового розгляду прокурору необхідно логічно інтегрувати докази електронної форми в структуру обвинувачення, забезпечуючи демонстрацію джерела походження, цілісності та зв'язку з юридично значущими обставинами, у разі потреби — із залученням спеціаліста. Технічні засади роботи мають відповідати вимогам ДСТУ ISO/IEC 27037:2017 та міжнародно визнаним методології належної фіксації даних з відкритих джерел.

10. Захисник у кримінальному провадженні виступає самостійним суб'єктом доказової діяльності щодо доказів електронної форми, реалізуючи гарантоване ч. 2 ст. 22 та ч. 3 ст. 93 КПК України право на їх використання. Ефективність цієї діяльності зумовлюється поєднанням процесуальної активності з технічною спроможністю забезпечити автентичність і цілісність цифрових даних (відповідно до ДСТУ ISO/IEC 27037:2017). На стадії обшуку й доступу до матеріалів (ст. 290 КПК України) пріоритетними є: мінімізація втручання у приватне життя, охорона адвокатської таємниці, вимога надання криміналістичних (побітових) копій і контрольних ідентифікаторів, а також своєчасного та ефективного реагування на процесуальні порушення.

11. Слідчий суддя та суд формують єдиний контур процесуального контролю за доказами електронної форми: перший – через попереднє санкціонування втручання у цифрове середовище і визначення обмежень щодо цифрових пристроїв, другий – через дослідження доказів електронної форми та перевірку їх належності, допустимості, достовірності та достатності. Ключовими орієнтирами є техніко-правові критерії: наявність у процесуальних документах і збіг геш-ідентифікаторів комп'ютерних даних, перевірюваність метаданих, відповідність процедур ідентифікації, збирання, здобуття та зберігання стандартам ДСТУ ISO/IEC 27037:2017. Перевага має надаватися криміналістичним (побітовим) копіям як об'єктам аналізу, тоді як дослідження оригінального пристрою допустиме лише за умов, що не створюють ризику цілісності доказу. Окремої уваги потребують електронні документи (включно з КЕП і позначкою часу), матеріали з відкритих джерел та докази, одержані за результатами міжнародної правової допомоги – перевірка їх походження та процесуальної легітимності.

12. У сучасному кримінальному процесі докази в електронній формі зумовлюють інституціалізацію спеціальних технічних знань і виокремлення автономних, але інтегрованих суб'єктів їх опрацювання — насамперед експертів, спеціалістів (з цифрової криміналістики, цифрової безпеки, OSINT-аналітиків та інших). Процесуальна роль експерта фокусується на науково вивіреному дослідженні, використанні атестованих методик та формулюванні висновку

експерта. Спеціаліст виконує технічну функцію «першої ланки» (DEFR): ідентифікація, фіксація, збереження та первинний аналіз цифрових слідів відповідно до ДСТУ ISO/IEC 27037:2017, із процесуальною фіксацією його участі й результатів. Чітке розмежування компетенцій цих суб'єктів оптимізує навантаження експертних установ і скорочує строки провадження; натомість їх змішування породжує процесуальні ризики перевантаження експертних установ та втрату релевантних цифрових даних. Залучення OSINT-аналітиків як спеціалістів для пошуку відомостей з відкритих джерел є доцільним за умови належної процесуальної фіксації та дотримання методології Протоколу Берклі.

13. Протокол Берклі забезпечує релевантну для кримінального процесу України методологію ведення розслідувань з використанням відкритих цифрових даних, поєднуючи організаційні, етичні й технічні стандарти. Їх впровадження покликане підвищити якість OSINT-матеріалів, знизити ризики визнання відповідних доказів недопустимими та посилити безпеку суб'єктів правозастосування. Для належної фіксації інформації з відкритого джерела під час кримінального провадження в протоколі огляду необхідно відобразити відомості, визначені в п. 155 Протоколу Берклі. Водночас варто зауважити розрив між практикою буквального використання терміна «Протокол Берклі» щодо таких протоколів огляду й реальним дотриманням його вимог, а також відсутність у КПК України уніфікованого процесуального порядку роботи з даними з відкритих джерел зумовлюють потребу нормативної деталізації. Судова рецепція Протоколу Берклі (2025) та рекомендації ОГП (2021) свідчать про позитивну динаміку, однак повноцінна інтеграція потребує поєднання нормативних змін, підготовки кадрів і матеріально-технічного забезпечення, що у підсумку сформує сталу технологію доказування в умовах цифровізації.

14. Конвенція про кіберзлочинність вибудовує цілісний процесуальний каркас міждержавної взаємодії у контексті роботи з доказами електронної форми. У КПК України відповідні інструменти частково імплементовано, однак зберігаються ключові прогалини: 1) знайшли відображення в КПК України: поширення обшуку за межі комп'ютерної системи, яка є об'єктом первинного втручання (ч. 2 ст. 19

Конвенції) – абз. 2 ч. 6 ст. 236 КПК України; 2) не імплементовано, але можуть бути реалізовані за допомогою існуючих процедур: термінове збереження комп'ютерних даних, які зберігаються (ст.ст. 16, 29), та порядок представлення (ст. 18) – частково через тимчасовий доступ до речей і документів (Глава 15 КПК України), перехоплення змісту даних, що передаються (ст. 21 Конвенції) – ст.ст. 263, 264 КПК України; 3) потребують імплементції в КПК України: термінове збереження і часткове розкриття даних про рух інформації (ст.ст. 17, 30), збирання даних про рух інформації у режимі реального часу (ст. 20); добровільне надання інформації (ст. 26). Другий додатковий протокол поглиблює співпрацю (прямі звернення до провайдерів, прискорені процедури, надзвичайні ситуації, стандарти захисту даних) і задає вектор подальшої гармонізації КПК України (після ратифікації).

Оптимальною вбачається комплексна імплементція: 1) кодифікація термінового збереження комп'ютерних даних, які зберігаються (ст.ст. 16, 29), термінового збереження і часткового розкриття даних про рух інформації (ст.ст. 17, 30), збирання даних про рух інформації у режимі реального часу (ст. 20); добровільного надання інформації (ст. 26); 2) процесуальна модель production order для комп'ютерних даних і відомостей про користувача; 3) чіткі гарантії пропорційності для збору трафіку в реальному часі та перехоплення контенту; 4) унормування взаємодії органів досудового розслідування з НКП 24/7. Системне впровадження цих механізмів забезпечить ефективність доказування з належним балансом прав людини й інтересів кримінального переслідування.

15. ISO/IEC 27037:2012, інтегрований у Європі як EN ISO/IEC 27037:2016 та імплементований в Україні через ДСТУ ISO/IEC 27037:2017, формує методологічне ядро поводження з доказами електронної форми: ідентифікація, збирання, здобуття (копіювання) та збереження із забезпеченням цілісності, відтворюваності й верифікованості. Українська правозастосовна практика, попри наявність указанного ДСТУ, стикається з нормативною лакуною КПК України щодо розмежування процесів ідентифікації, збирання та здобуття доказів електронної форми, процесуального закріплення ролей DEFR та DES, фіксації ланцюга збереження тощо. Необхідними заходами в цьому напрямі визначено таке: 1) процесуальна

легітимація основних підходів ДСТУ ISO/IEC 27037:2017 у КПК України; 2) відображення процедур ДСТУ ISO/IEC 27037:2017 в СОП; 3) інституціоналізація ролей DEFR та DES і вимог до їх компетентності; 4) системне навчання оперативних працівників, слідчих та прокурорів роботі з доказами електронної форми відповідно до вимог ДСТУ ISO/IEC 27037:2017 для можливості виконання функцій DEFR.

16. Порівняльний аналіз зарубіжного досвіду засвідчує, що докази електронної форми перетворилися на системоутворювальний елемент кримінального провадження, а ефективність їх використання зумовлюється поєднанням чітких процесуальних рамок, інституційної спроможності та транснаціональної взаємодії. ЄС запроваджує наднаціональну модель (пакет e-evidence) з прямою адресацією до провайдерів і вбудованими гарантіями прав людини, англо-американські юрисдикції забезпечують гнучкість через прецедент і професійні стандарти, натомість континентальні системи формують детальні механізми процесуального контролю. Основні виклики у цій сфері проявляються через колізії юрисдикцій, потребу підтвердження автентичності даних та фіксації ланцюга збереження доказів, загрози кібербезпеки і потребу стандартизації процесуальних процедур.

Варто визначити тенденції зарубіжного досвіду правового регулювання щодо досліджуваного предмета, серед яких: інституціоналізація правового режиму доказів електронної форми у межах кримінального процесуального законодавства; утвердження технологічно нейтрального підходу до їх оцінки та допустимості (відсутність вимог визначених технічних засобів чи форматів); посилення вимог до автентичності, цілісності й простежуваності; запровадження спеціальних процесуальних механізмів для їх збирання, збереження та перевірки; уніфікація національних підходів із міжнародними стандартами.

У сфері міжнародного обміну доказами електронної форми перспективними напрямами розвитку є: 1) створення комплексної та надійної системи їх захисту; 2) розроблення й уніфікації стандартних протоколів та процедур для гармонізації правових аспектів обміну доказами електронної форми між різними юрисдикціями; 3) впровадження сучасних систем управління доказами, що забезпечують автоматизовану фіксацію, відстеження та аналіз усіх взаємодій з ними.

17. Удосконалення організаційних засад роботи з доказами електронної форми є важливим чинником адаптації кримінального процесу України до цифрової доби. Ефективність цього напряму визначається рівнем матеріально-технічного забезпечення суб'єктів кримінального провадження, наявністю кваліфікованих кадрів і спроможністю до міжвідомчої взаємодії. Підготовка спеціалізованих кадрів, створення криміналістичних ІТ-лабораторій, а також впровадження міждисциплінарних програм навчання формують основу інституційної спроможності системи кримінальної юстиції. Стандартизація діяльності суб'єктів кримінального провадження через розроблення СОП забезпечує єдність практики, передбачуваність дій і зменшує ризики втрати чи спотворення доказів. Водночас розбудова системи міжвідомчої координації, цифровізації процедур тимчасового доступу до речей і документів та створення захищених цифрових сховищ, підтвердження цілісності даних шляхом фіксації їх геш-ідентифікаторів, запровадження обов'язкового резервного копіювання та криптографічного захисту сприяють збереженню цілісності та конфіденційності доказів електронної форми.

18. Процесуальне вдосконалення роботи з доказами електронної форми передбачає розвиток нормативної бази зі збереженням балансу між правовою визначеністю та технічною адаптивністю, запобіганням надмірній формалізації процедур і, водночас, гарантуванням автентичності, цілісності і допустимості доказів цієї категорії. Запропоновані зміни до КПК України передбачають поетапне впровадження міжнародних стандартів Конвенції про кіберзлочинність та актів ЄС. Визначальним є закріплення базових дефініцій, унормування ідентифікації комп'ютерних даних на основі їх гешування, створення цифрових архівів, впровадження практики фіксації ланцюга збереження доказів (chain of custody), регламентації «віртуального огляду» та використання його результатів як доказів та інше. Поетапне запровадження відповідних положень має супроводжуватися навчанням суб'єктів кримінального провадження, розробленням СОП і створенням міжвідомчих механізмів координації.

19. Технічне вдосконалення роботи з доказами електронної форми спрямоване на ефективне їх використання і потребує створення інфраструктури, що охоплює

сертифіковані системи ідентифікації та зберігання. Упровадження цифрових протоколів слідчих дій, резервного копіювання та централізованих сховищ із багаторівневим шифруванням забезпечує збереження й контрольованість електронних даних протягом усього процесуального циклу. Використання геш-ідентифікаторів комп'ютерних даних як процесуального реквізиту протоколу слідчих (розшукових) дій, підкріпленого кваліфікованим електронним підписом, створює об'єктивний механізм перевірки автентичності та цілісності доказів електронної форми. Уніфікація технічних вимог, сертифікація програмних засобів і нормативне закріплення процедур цифрової обробки доказів електронної форми становлять основу для формування цілісної державної політики у відповідній сфері.

20. Концепція вдосконалення інституту доказів електронної форми у кримінальному процесі України спрямована на створення єдиного науково обґрунтованого та технологічно інтегрованого механізму їх процесуального обігу. Її сутність полягає у комплексному розвитку нормативних, організаційних, інфраструктурних, техніко-криміналістичних, освітніх та науково-аналітичних напрямів. Концепція передбачає законодавче унормування критеріїв їх допустимості, установлення уніфікованого порядку їх ідентифікації, фіксації та дослідження. Інфраструктурний та техніко-криміналістичний компоненти передбачають стандартизацію форматів зберігання, сертифікацію програмних засобів і створення інтегрованої системи управління доказами, синхронізованої з національними реєстрами. Освітній напрям орієнтований на фахову підготовку суб'єктів кримінального провадження, а науково-аналітичний – на запровадження постійного аналізу стану правозастосування й оновлення методичних стандартів. Реалізація цієї концепції забезпечить підвищення ефективності електронного сегменту доказування, зміцнить гарантії прав учасників процесу та гармонізує національну практику з міжнародними стандартами кримінальної юстиції.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авдєєва Г. К. Проблеми визначення достовірності цифрових доказів у кримінальному провадженні. *Вісник ЛННІ ім. Е. О. Дідоренка*. 2024. Вип. 1 (105). С. 33–39. URL: http://nbuv.gov.ua/UJRN/Tpsek_2023_1_9.
2. Авдєєва Г. К. Сліди злочинів у сфері використання інформаційних технологій: способи виявлення. *Питання боротьби зі злочинністю*. 2015. Вип. 30. С. 88–98. URL: http://nbuv.gov.ua/UJRN/Pbzz_2015_30_10.
3. Авдєєва Г. К. Стороженко С. В. Електронні сліди : поняття та види. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2017. Вип. 1. С. 168–175. URL: http://nbuv.gov.ua/UJRN/Vlduvs_2017_1_21.
4. Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*. 2023. Вип. 1. С. 126–143. URL: http://nbuv.gov.ua/UJRN/Tpsek_2023_1_9.
5. Академічний тлумачний словник української мови. URL: <http://sum.in.ua/s/pysjmovuj>.
6. Актуальні питання призначення та проведення експертизи: наук.-практ. посіб.; за заг. ред. І. І. Присяжнюка. К. Національна академія прокуратури України, 2017. 300 с.
7. Алексєєва-Процюк Д. О., Брисковська О. М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. 2018. Вип. 2. С. 247–253.
8. Ангеленюк А.-М. Ю. 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.

9. Андреев І. П. Доктринальний аналіз поняття та змісту формування доказів адвокатом у кримінальному провадженні. *Juris Europensis Scientia*. 2025. Вип. 1. С. 102–106. URL: <https://doi.org/10.32782/chem.v1.2025.19>.
10. Антонюк А. Б., Русецька В. А. Електронні докази в кримінальному провадженні. *Міжнародний науковий журнал «Інтернаука»*. 2020. № 10. С. 78–87.
11. Антощук А. О., Гриненко К. В. Особливості пред'явлення особи для впізнання за матеріалами відеозапису. *Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 18: Право*. № 36. 2021. С. 3–9. URL: <http://enpuir.npu.edu.ua/handle/123456789/36653>.
12. Ахтирська Н. М. Одержання доказів в електронній формі в світлі Другого додаткового протоколу до Конвенції про кіберзлочинність. *Криміналістика і судова експертиза*. 2022. Вип. 67. С. 188–200.
13. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2016. Вип. 36(2). С. 123–125.
14. Бабаєва О. В., Авербах Д. В. Щодо питання про використання доказів, отриманих з відкритих джерел, у кримінальному провадженні. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО*. 2024. Вип. 83. Ч. 3. С. 169–174.
15. База правових позицій Верховного Суду. URL: <https://lpd.court.gov.ua>.
16. Барабаш А. А., Клепка Д. І. Нормативні підходи до визначення електронних доказів та порядку їх подання у процесуальному законодавстві. *Перспективні напрями розвитку кримінальної юстиції в цифрову еру* : матеріали всеукр. заоч. наук.-практ. конф. (м. Харків, 24 лип. 2023 р.). Харків, 2023. С. 29–34.
17. Басай В. Д., Томин С. В. Дослідження віртуальних слідів – перспективний напрямок криміналістичного слідознавства. *Актуальні проблеми держави і права*. Одеса, 2008. Вип. 44. С. 220–223. URL: http://nbuv.gov.ua/UJRN/apdp_2008_44_44.

18. Басиста І. В., Гаврилук Л. В., Гутник А. В., Хитра А. Я. Використання цифрових даних з відкритих джерел під час розслідування кримінальних правопорушень: окремі аспекти. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія Право*. Івано-Франківськ : Редакційно-видавничий відділ Університету Короля Данила, 2024. Вип. 17 (29). С. 227–243. URL: <https://doi.org/10.33098/2078-6670.2024.17.29.227-243>.
19. Басюк Л., Антощук А. Організація та тактика використання 3D-сканування під час огляду місця події. *Український політико-правовий дискурс*. 2025. Вип. 8. URL: <https://doi.org/10.5281/zenodo.14982555>.
20. Бистрова Ю. В. Інноваційні методи навчання у вищій школі України. *Право та інноваційне суспільство*. 2015. № 1. С. 27–33.
21. Біленчук П. Д. Криміналістична тактика і методика розслідування окремих видів злочинів : навч. посіб. / П. Д. Біленчук, А. П. Гель, Г. С. Семаков. Київ : МАУП, 2007. 512 с.
22. Білецький А., Цапок М. Правові аспекти введення електронної системи управління кримінальними провадженнями (e-Case Management System) у кримінальний процес щодо корупційних правопорушень. Київ : ТОВ РЕД ЗЕТ, 2020. 32 с. URL: <https://ekmair.ukma.edu.ua/handle/123456789/20892>.
23. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : автореф. дис. ...канд. юрид. наук. Київ, 2008. 18 с.
24. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання : монографія. Львів : ЛьвДУВС, 2020. 256 с. URL: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/3337/1/%d0%91%d0%bb%d0%b0%d0%b3%d1%83%d1%82%d0%b0--%d0%9c%d0%be%d0%b2%d1%87%d0%b0%d0%bd--%d0%bc%d0%be%d0%bd%d0%be%d0%b3%d1%80%d0%b0%d1%84%d1%96%d1%8f--%d0%92%d0%95%d0%a0%d0%a1%d0%a2%d0%9a%d0%90.pdf>.

25. Браун С., Овсянніков В. С., Шинкоренко С. В. Застосування електронних доказів під час розгляду справ, пов'язаних з корупцією : збірка навчальних матеріалів тренінгу для суддів. 2019. 138 с. URL: <http://www.nsj.gov.ua/files/1581330611%D0%9F%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%20%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D1%96%20%D0%B4%D0%BE%D0%BA%D0%B0%D0%B7%D0%B8%202019.pdf>.

26. Вапнярчук В. В. Теоретичні основи кримінального процесуального доказування : дис. ... д-ра юрид. наук : 12.00.09; Нац. юрид. ун-т ім. Ярослава Мудрого, М-во освіти і науки України. Харків, 2018. 509 с.

27. Вапнярчук В. В. Теорія і практика кримінального процесуального доказування : монографія. Харків : Юрайт, 2017. 408 с.

28. Вернидубов І., Белікова С. Електронні докази: поняття, особливості та проблеми щодо їх дослідження судом. *Evropský politický a právní diskurz*. 2018. Sv. 5, Vyd. 2. С. 299–305. URL: http://nbuv.gov.ua/UJRN/evrpol_2018_5_2_42.

29. Вибір заради справедливості : посібник зі створення механізмів притягнення до відповідальності за найтяжчі злочини. Т. 2. / пер. О. Бондаренко; заг. ред. Р. Мартиновський, Л. Мороз. Переклад та видання здійснене за підтримки Програми «Права людини і правосуддя» Міжнародного фонду «Відродження». 2018. 544 с. URL: https://www.irf.ua/wp-content/uploads/2020/06/tom_ii_web.pdf.

30. Використання електронних (цифрових) доказів у кримінальних провадженнях : методичні рекомендації / М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін. ; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

31. Використання електронних (цифрових) доказів у кримінальних провадженнях : методичні рекомендації / М. В. Гребенюк, В. Д. Гавловський, М. В. Гуцалюк, В. Г. Хахановський та ін. ; за заг. ред. М. В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 76 с.

32. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів : методичні рекомендації / авт. колектив: А. В. Захарко, А. Г.

Гаркуша, В. В. Рогальська, І. В. Краснобрижний, О. В. Брягін / Дніпро : Дніпропетровський державний університет внутрішніх справ, 2019. 73 с. URL: <http://er.dduvs.edu.ua/handle/123456789/3885>.

33. Вілінський М. Електронний висновок експерта: теоретичні основи та практичний аспект. *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки*. 2023. № 2 (126). С. 10–19. URL: <https://doi.org/10.17721/1728-2195/2023/2.126-2>.

34. Власова Г. П., Каланча І. Г. Захисник як суб'єкт роботи з електронними доказами в кримінальному провадженні. Актуальні питання реформування правової системи : зб. матеріалів XXII Міжнар. наук.-практ. конф., Луцьк, 13-15 червня 2025 р. / Уклад. Джурак Л. М. – Луцьк : Вежа-Друк, 2025. С. 113-115. URL: https://www.law.vnu.edu.ua/_files/ugd/65dd18_5ab2de833d004115b0483aa2420d7cc0.pdf.

35. Волков О. О. Основні джерела криміналістично-значимої інформації про злочини пов'язані з шкідливими програмними засобами. *Innovative solutions in modern science*. 2018. № 3 (22). 15 с.

36. Воробчак А. Р. Висновок експерта як джерело доказів у кримінальному провадженні : дис. ... канд. юрид. наук : 12.00.09. Одеса, 2019. 236 с.

37. Вступ до цифрової криміналістики : навч. посіб. / В. Ю. Шепітько, К. В. Латиш, М. В. Капустіна, С. С. Демидова ; за ред. В. Ю. Шепітька; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2025. 124 с.

38. Гавриш О. С., Чепинога А. В., Гончаров А. В., Катаєв Д. С. Організаційна структура захисту розподіленої мережі підприємства на основі шлюзів безпеки CISCO. *Вісник ХНУ. Хмельницький*, 2025. №5.2. URL: <https://doi.org/10.31891/2307-5732-2025-357-99>.

39. Гавриш Т. С. Проблеми допустимості доказів, отриманих в ході міжнародної правової допомоги в кримінальних справах : дис. ... канд. юрид. наук: 12.00.09. Харків, 2004. 224 с.

40. Гарасимів О., Марко С., Ряшко О. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий*

вісник Ужгородського Національного Університету. Серія ПРАВО. 2023. Вип. 75, ч. 2. С. 158–162. URL: <https://doi.org/10.24144/2307-3322.2022.75.2.25>.

41. Гаркуша А. М. Використання геш-функції для ідентифікації комп'ютерних даних та перевірки їх цілісності. Криміналістика та судова експертиза: сучасний стан і перспективи розвитку : матеріали Всеукр. наук.-практ. конф. (м. Київ, 05 груд. 2024 р.). Київ : ДНДЕКЦ МВС України, 2024. С. 89–93.

42. Гаркуша А. М. Використання кваліфікованої електронної позначки часу для фіксації комп'ютерних даних у кримінальному провадженні. *Проблеми державотворення і захисту прав людини в Україні* : матеріали XXXI звітної наук.-практ. конф. (м. Львів, 6–7 лют. 2025 р.). Львів : Юридичний факультет Львівського національного університету імені Івана Франка, 2025. С. 501–503. URL: https://www.researchgate.net/publication/388818545_Vikoristanna_kvalifikovanoi_elektronnoi_poznacki_casu_dla_fiksacii_komp%27uternih_danih_u_kriminalnomu_provadzenni.

43. Гаркуша А. М. Допустимість і достовірність електронних документів у кримінальному провадженні. *Теоретико-прикладні проблеми юридичної науки на сучасному етапі реформування кримінальної юстиції* : зб. тез Міжнар. наук.-практ. конф. (м. Хмельницький, 10 трав. 2024 р.). Хмельницький, 2024. С. 73–77.

44. Гаркуша А. М. Допустимість і достовірність резервних копій комп'ютерних даних. *III Наукові читання пам'яті Ганса Гросса* : зб. тез Міжнар. наук.-практ. конф. (м. Чернівці, 08 груд. 2023 р.). Чернівці : Чернівець. нац. ун-т. ім. Ю. Федьковича, 2023. С. 43–47.

45. Гаркуша А. М. Стратегії та засоби подолання систем логічного захисту доступу до комп'ютерних систем. *Криміналістика та судова експертиза у XXI столітті* : матеріали Всеукр. наук.-практ. семінару (м. Київ, 30 трав. 2024 р.). Київ : ДНДЕКЦ МВС України, 2024. С. 57–61.

46. Гаркуша А. М., Каланча І. Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи* : матеріали круглого столу (м. Львів, 11 черв. 2021 р.). Львів : Львівський державний університет внутрішніх справ, 2021. С. 159–165.

URL:

https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/11_06_2021.pdf.

47. Гаркуша А. М., Каланча І. Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. *Наукові читання пам'яті Ганса Гросса* : зб. тез Міжнар. наук.-практ. конф. (м. Чернівці, 09 груд. 2021 р.). Чернівці : Технодрук. С. 72–75. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/11383/Forensic_Epistemology_Czernowitz_2021_.pdf?sequence=1&isAllowed=y.

48. Гафич О. І. Цифровізація доказової бази у кримінальному провадженні: роль адвоката в забезпеченні прав підзахисного. *Юридичний науковий електронний журнал*. 2024. № 12. С. 340–343. URL: <https://doi.org/10.32782/2524-0374/2024-12/78>.

49. Гвоздік О. І., Старенький О. С. Логіка формування доказової бази в кримінальному провадженні. *Філософські та методологічні проблеми права*. 2022. № 2 (24). С. 56–63. URL: <https://philosophy.navs.edu.ua/index.php/philosophy/article/view/1514/1508>

50. Глинська Н. В., Клепка Д. І. Основні аспекти стратегії унормування інститутицифрових доказів в кримінальному процесуальному законодавстві. *Питання боротьби зі злочинністю*. 2023. Вип. 46. С. 48–66.

51. Глібко В. М. Роль документів у розслідуванні злочинів. *Теорія і практика правознавства*. 2016. № 1. С. 1–11.

52. Гмирко В. П. Доказування в кримінальному процесі: діяльнісна парадигма. Теоретичний аналіз. Проблематизація. СМД-репрезентація. Дніпропетровськ : Академія митної служби України, 2010. 314 с. URL: <http://biblio.umsf.dp.ua/jspui/bitstream/123456789/2151/1/Монографія.PDF>

53. Гмирко В. П. Кримінально-судові докази: юридичне поняття чи дефініція. *Право України*. 2014. № 10. С. 26–35.

54. Гонгало С. Й. Електронні документи як об'єкти судової техніко-криміналістичної експертизи та їх класифікація. *Адвокат*. 2013. № 1 (148). С. 33–36.

55. Гонгало С. Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку : дис. ... канд. юрид. наук : 12.00.09 / Київський національний університет ім. Т. Шевченка. Київ, 2013. 190 с.
56. Гонгало С. Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку : автореф. дис. ... канд. юрид. наук : 12.00.09 / Київський національний університет ім. Т. Шевченка. Київ, 2013. 21 с.
57. Гора І. В., Колесник В. А., Попович І. І. До питання про цифрову криміналістику в системі криміналістичних знань. *Науковий вісник МГУ. Юриспруденція*. 2024. № 68. С. 86–91. URL: <https://doi.org/10.32782/2307-1745.2024.68.18>.
58. Гора І. В. Цифрова криміналістика в системі знань слідчих і оперативних працівників Служби безпеки України. *Посилення спроможностей СБ України та взаємодія зі складовими сектору безпеки і оборони* : матеріали конф. (м. Київ, 27 вересня 2024 р.). Київ : НА СБУ, 2024. С. 65–68.
59. Гора І. В., Колесник В. А. Актуальні питання криміналістичного забезпечення досудового розслідування злочинів проти інформаційної безпеки держави. *Криміналістика і судова експертиза* : міжвідом. наук.-метод. зб. Вип. 69. С. 167–175. Київ : Вид-во Ліра-К, 2024. 1033994/kndise.2024.69.02.
60. Гора І. В., Колесник В. А., Попович І. І. Цифрова криміналістика в забезпеченні діяльності з протидії злочинності. *Науковий вісник УжНУ. Серія Право*, 2024. № 85. Ч. 4. С. 63–70. URL: <https://doi.org/10.24144/2307-3322.2024.85.4.9.c.63-70>.
61. Горбенко Г. Пошук інформації в базах даних : посібник з курсу. Київ, 2022. 259 с. URL: <https://acrec.org.ua/wp-content/uploads/2023/02/handbook.pdf>.
62. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика. Застосування : монографія. Харків : Видавництво «Форт», 2012. 870 с.
63. Гребенькова М. С. Належність і допустимість електронних відображень як джерел доказів у кримінальному провадженні. *Юридичний*

науковий електронний журнал. 2021. № 12. С. 335–338. URL: <https://doi.org/10.32782/2524-0374/2021-12/84>.

64. Гусєв О. Ю. Правомірність доступу до цифрових даних як умова допустимості електронних доказів. *Часопис Київського університету права*. 2019. № 1. С. 148–151. URL: <https://chasprava.com.ua/index.php/journal/article/view/210>.

65. Давидюк П. П., Кубай І. Ю. Висунення і перевірка слідчих версій про цифрове алібі підозрюваного (обвинуваченого). *Молодий вчений*. 2017. № 5 (45). С. 29–32.

66. Дегтярьова О. Доказування у кримінальному провадженні на підставі електронних доказів. *Юридичний вісник. Одеса : Гельветика*. 2021. № 6. С. 273–278. URL: <https://dspace.onua.edu.ua/server/api/core/bitstreams/095378c2-e142-42c6-bd3e-14adeff1f84f/content>.

67. Демура М. І., Клепка Д. І., Крицька І. О. Забезпечення прав та законних інтересів особи в умовах «діджиталізації» кримінального провадження. *Часопис Київського університету права*. № 1. С. 295–301. URL: <https://doi.org/10.36695/2219-5521.1.2020.59>.

68. Дехтяр О. Г. Засада безпосередності дослідження показань, речей і документів та її реалізація у кримінальному провадженні : автореф. дис. ... канд. юрид. наук : 12.00.09. Нац. ун-т «Одес. юрид. акад.». Одеса, 2014. 20 с.

69. Деякі питання документування управлінської діяльності : Постанова Кабінету Міністрів України від 17.01.2018 р. № 55 (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/main/55-2018-%D0%BF?utm>.

70. Деякі питання електронної ідентифікації та електронних довірчих послуг : Постанова Кабінету Міністрів України від 28.06.2024 р. № 764. URL: <https://zakon.rada.gov.ua/laws/show/764-2024-п>.

71. Джордж Е., Меріда Ф; Расмуссен У., Волзов В., Джонс Н. Посібник з питань електронних доказів : базовий посібник для співробітників правоохоронних органів, прокурорів та суддів. Версія 2.1. Відділ протидії кіберзлочинності. Генеральний директорат з прав людини та верховенства права. Страсбург, Франція. 2020. 218 с.

72. Дикий О. В., Сидорчук В. В. Поняття OSINT та суміжні категорії. *Юридичний науковий електронний журнал*. № 9. 2024. С. 332–335.
73. Доказування у кримінальному провадженні : курс лекцій / О. О. Бондаренко, Г. І. Глобенко, В. В. Романюк та ін. ; за заг. ред. О. О. Юхна ; МВС України, Харків. нац. ун-т внутр. Харків : ХНУВС, 2018. 156 с.
74. Доказування у кримінальному провадженні : навч.-практ. посіб. / кол. авт. Київ : Національна академія прокуратури України, 2017. 346 с.
75. Допустимість, оброблення та ланцюг зберігання електронних доказів для суддів і прокурорів України. Національна школа суддів України. URL: <https://nsj.gov.ua/ua/news/dopustimist-obroblennya-ta-lantsug-zberigannya-elektronnih-dokaziv-dlya-suddiv-i-prokuroriv-ukraini/>.
76. ДСТУ 2227–93 «Системи оброблення інформації. Автоматизована установа. Терміни та визначення». Київ : Держстандарт України, 1993. 17 с.
77. ДСТУ 2732:2004 «Діловодство й архівна справа. Терміни та визначення понять», затверджений Наказом від 28.05.2004 № 97 Про затвердження національних стандартів України, державних класифікаторів України, національних змін до міждержавних стандартів, внесення зміни до наказу Держспоживстандарту України від 31.03.2004 р. № 59 та скасування нормативних документів. URL: [https://vn.court.gov.ua/userfiles/27_2732-2004\(1\).pdf](https://vn.court.gov.ua/userfiles/27_2732-2004(1).pdf).
78. ДСТУ 4163:2020 «Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів». 37 с. URL: <https://www.kdu.edu.ua/Documents/DSTU41632020v1.pdf?utm>.
79. ДСТУ 7157:2010. Інформація та документація. Видання електронні. Основні види та вихідні відомості. Чинний від 01.07.2010. Вид. Офіц. Київ, Держспоживстандарт України, 2010. 14 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTY1/dsty_7157-2010.pdf.
80. ДСТУ 7448:2013: Інформація та документація. Бібліотечно-інформаційна діяльність. Терміни та визначення понять. Київ : Мінекономрозвитку України, 2014. 41 с.

81. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція гешування. Чинний від 01.04.2015. Вид. офіц. Київ : ДП «УкрНДНЦ», 2015. 34 с.

82. ДСТУ ETSI TS 119 312:2022 (ETSI TS 119 312 V1.4.2 (2022-02), IDT). Електронні підписи та інфраструктури (ESI). Криптографічні пакети. Чинний від 01.01.2023. Вид. офіц. 30 с.

83. ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. Чинний від 01.01.2019. Київ : УкрНДНЦ, 2018. 31 с.

84. Дубняк К. А. Інформаційний простір: структура та функціональні параметри. *Держава та регіони. Серія: Соціальні комунікації*. 2015. № 4 (24). С. 21–25.

85. Дудич А. В. Експерт як учасник кримінального провадження : дис. ... канд. юрид. наук : 12.00.09. Одеса, 2017. 253 с. URL: <https://dspace.onua.edu.ua/server/api/core/bitstreams/85e1e0bd-8853-4bd3-ad1d-4fe4af3a07c8/content>.

86. Електронні докази у кримінальному провадженні: поняття, збирання, використання в доказуванні : монографія / І. В. Гора, В. А. Колесник, В. В. Малюк, В. О. Ходанович, А. М. Черняк, Л. І. Щербина ; за заг. ред. В. А. Колесника. Київ : 7БЦ, 2024. 484 с.

87. Єдиний державний реєстр судових рішень. URL: <https://reyestr.court.gov.ua/>

88. Запотоцький А. П. Документи як процесуальні джерела доказів у кримінальному судочинстві : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2009. 26 с.

89. Зінченко В.М. Достатність доказів у кримінальному провадженні: дис. ... канд. юрид. наук: 12.00.09. Одеса, 2020. 231 с. URL: <https://hdl.handle.net/11300/13757>.

89. Зозуля Н. Електронні чи цифрові докази: удосконалення змін до процесуального законодавства. *Українське право*. 08.05.2018. URL:

https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazydoskonalennya_zmin_do_protseualnogo_zakonodavstva.

90. Інструкція про призначення та проведення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 08.10.1998 р. № 53/5 (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/show/z0705-98#n14>.

91. Інформаційний лист Особливості призначення та можливості судової комп'ютерно-технічної експертизи. Київський науково-дослідний експертно-криміналістичний центр МВС України. Київ, 2023. 5 с. URL: https://ndekc.kiev.ua/wp-content/uploads/2023/01/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE-%D1%82%D0%B5%D1%85%D0%BD%D1%96%D1%87%D0%BD%D0%B0-%D0%B5%D0%BA%D1%81%D0%BF%D0%B5%D1%80%D1%82%D0%B8%D0%B7%D0%B0_.pdf?utm.

92. Кайло І. Ю. Допустимість доказів у кримінальному процесі України : дис. ... канд. юрид. наук : 12.00.09. Харків, 2016. 218 с.

93. Каланча І. Г. Алгоритм електронного кримінального провадження. *Law. State. Technology*, 2024. Вип. 4, С. 69–74. URL: <https://doi.org/10.32782/LST/2024-4-13>.

94. Каланча І. Г. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світлі концепції chain of custody. *Věda a perspektivy*. № 8(51) (2025). С. 206-230. URL: https://www.researchgate.net/publication/394998880_Kalanca_IG_Dokazi_so_maut_elektronnu_formu_v_kriminalnomu_procesi_Ukraini_identifikacia_ta_cilisnist_u_svitli_koncepcii_chain_of_custody_Veda_a_perspektivy_No_851_2025_C_206-230.

95. Каланча І. Г. Електронне кримінальне судочинство: передумови виникнення, сучасний стан та перспективи розвитку : монографія. Харків : Право, 2018. 240 с. URL: https://www.researchgate.net/publication/389613007_Kalanca_I_G_Elektronne_krimin

alne_sudocinstvo_peredumovi_viniknenna_sucasnij_stan_ta_perspektivi_rozvitku_monografia_Harkiv_Pravo_2018_240_s_ISBN_978-966-937-546-9.

96. Каланча І. Г. Електронний висновок експерта як доказ у кримінальному процесі України: практика, перспективи та ризики. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. № 2. С. 84–92. URL: <https://doi.org/10.32782/2311-8040/2025-2-12>.

97. Каланча І. Г. Електронний сегмент в кримінальному процесі Грузії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. № 4. 2019. С. 161–166. URL: <https://doi.org/10.31733/2078-3566-2019-4-161-166>.

98. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законодавстві Молдови. *Jurnalul Juridic National: teorie si practica*. № 1(41). 2020. С. 132–137. URL: <http://www.jurnaluljuridic.in.ua/archive/2020/1/30.pdf>.

99. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Азербайджану. *Науковий вісник Ужгородського національного університету. Серія «Право»*. № 59. 2019. С. 117–121. URL: <https://doi.org/10.32782/2307-3322.59-2.26>.

100. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Туркменістану. *Актуальні проблеми вітчизняної юриспруденції*. 2020. № 1. С. 91–95. URL: http://apnl.dnu.in.ua/1_2020/23.pdf.

101. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Вірменії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2020. № 1. С. 205–210. URL: <https://doi.org/10.31733/2078-3566-2020-1-205-210>.

102. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Латвії. *Криміналістика і судова експертиза : міжвідомчий науково-методичний збірник*. 2020. Вип. 65. С. 90–100. URL: <https://doi.org/10.33994/kndise.2020.65.09>.

103. Каланча І. Г. Електронний сегмент кримінального процесу Естонії. *Порівняльно-аналітичне право*. 2019. № 3. С. 212–216. URL: https://pap-journal.in.ua/wp-content/uploads/2021/07/3_2019.pdf.

104. Каланча І. Г. Єдине електронне інформаційне поле органів кримінальної юстиції. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : матеріали Міжнар. наук.-практ. конф. (м. Київ, 5 листоп. 2019 р.). Київ, 2019. С. 209-213.

105. Каланча І. Г. Інтєроперабельність як обов'язкова властивість електронних інформаційних систем органів кримінальної юстиції. *Ročenka Ukrajinsko-Slovenská. Zborník vedeckých prác. (Рочник Українсько-Словацький. Збірник наукових праць)*. 2020. С. 64–70. URL: <https://www.eeda.sk/dok/publikacie/ostatne/2020-rocenka-ukrajinsko-slovenska.pdf>.

106. Каланча І. Г. Кіберпростір як територія проведення досудового розслідування. *Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини* : збірник наук. праць за матеріалами Круглого столу (м. Київ, 7 груд. 2023 р.). Київ : Київ. стол. ун-т ім. Б. Грінченка, 2024. С. 115–119. URL: <https://kubg.edu.ua/struktura/pidrozdili/yurydychna-klinika-astreya/zakhody/8438-ikh-kruhlyi-stil-prava-liudyny-v-umovakh-voiennoho-stanu-v-ukraini.html>.

107. Каланча І. Г. Матеріальна форма існування як властивість доказу в кримінальному процесі України: практика правозастосування. *Права людини в умовах воєнного стану в Україні* : Х круглий стіл до Всеукр. тижня права (м. Київ, 10 груд. 2024 р.). Київ : Київ. столич. ун-т ім. Б. Грінченка, 2025. С. 63–67.

108. Каланча І.Г. Методологія дослідження електронної складової кримінальної процесуальної діяльності. *Науковий часопис Національної академії прокуратури України*. №2. 2018. С. 59-68.

109. Каланча І. Г. Окремі аспекти діяльності прокурора щодо гарантування цілісності доказів, що мають електронну форму під час досудового розслідування кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні* : матеріали VI Міжнар. наук.-практ. конф. (м. Чернівці, 21 жовт. 2022 р.). Чернівці, 2022. С. 327–332. URL: https://ccu.gov.ua/sites/default/files/suchasni_vyklyky_ta_aktualni_problemy_sudovoyi_reformy_v_ukrayini_2022.pdf.

110. Каланча І. Г. Організаційні аспекти роботи з доказами, що мають електронну форму в кримінальному процесі України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. Вип. 90, Ч. 4. 2025. С. 258-266. URL: <https://doi.org/10.24144/2307-3322.2025.90.4.36>.

111. Каланча І. Г. Організація навчання представників органів кримінальної юстиції сучасним процесуально-цифровим компетентностям. Training legal professionals following European standarts: scientific and pedagogical internship (Riga, November 4–December 15, 2024). Riga, the Republic of Latvia, 2024. p.p. 45-50.

112. Каланча І. Г. Підходи до класифікації електронних носіїв інформації та інформаційних систем для завдань кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні* : матеріали V Міжнар. наук.-практ. конф. (м. Чернівці, 29 жовт. 2021 р.). Чернівці, 2021. С. 211–213. URL: <https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk-29.10.21.pdf>.

113. Каланча І. Г. Поняття практики Європейського суду з прав людини як джерела кримінального процесуального права України. *Вісник кримінального судочинства*. 2020. № 2. С. 8–21. URL: https://vkslaw.knu.ua/images/verstka/Visnyk_Krim_Sud_3-4_20_231013_avt-8-21.pdf.

114. Каланча І. Г. Практика роботи з доказами, що мають електронну форму в кримінальному процесі України: соціологічне дослідження. *Успіхи і досягнення у науці*. 2025. № 1 (11). С. 76–93. URL: [https://doi.org/10.52058/3041-1254-2025-1\(11\)-76-93](https://doi.org/10.52058/3041-1254-2025-1(11)-76-93).

115. Каланча І. Г. Процесуальна природа доказів, що мають електронну форму в кримінальному процесі України: документ та речовий доказ. *Міжнародний науковий журнал "Інтернаука". Серія: "Юридичні науки"*. № 7. 2025. С. 85-92. DOI <https://doi.org/10.25313/2520-2308-2025-7-11208> URL: <https://www.inter-nauka.com/uploads/public/17557614844770.pdf>.

116. Каланча І. Г. Результати OSINT як джерело доказів у кримінальному процесі України. *Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій* : Всеукр. наук.-практ. конф. (м. Чернівці, 20 груд. 2024 р.). Чернівці, 2024.

117. Каланча І. Г. Роль правових актів Європейського суду з прав людини в кримінальному процесі України. *Проблеми законності*. 2020. № 150. С. 233–243. URL: <https://doi.org/10.21564/2414-990x.150.209071>.

118. Каланча І. Г. Способи ідентифікації комп'ютерних даних як доказу в кримінальному провадженні. *III Наукові читання пам'яті Ганса Гросса* : збірник тез Міжнар. наук.-практ. конф. (м. Чернівці, 08 груд. 2023 р.). Чернівці : Чернівець. нац. у-нт. ім. Ю. Федьковича, 2023. С. 71–75. URL: <https://www.ndekc.cv.ua/wp-content/uploads/2024/03/III-Naukovi-chytannya-pam-yati-Gansa-Grossa.pdf>.

119. Каланча І. Г. Стратегії фіксації доказів, що мають електронну форму для застосування в кримінальному провадженні. *Сучасні виклики та актуальні проблеми судової реформи в Україні* : матеріали VII Міжнар. наук.-практ. конф. (м. Чернівці, 27 жовт. 2023 р.). Чернівці, 2023. С. 253–258. URL: https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk_conf_27..pdf.

120. Каланча І. Г. Судове провадження в умовах електронного реформування кримінальної юстиції України : дис. ... канд. юрид. наук : 12.00.09. Київ, 2017. 277 с. URL: https://www.researchgate.net/publication/389623453_Kalanca_I_G_Sudove_provadzen_na_v_umovah_elektronnogo_reformuvanna_kriminalnoi_usticii_Ukraini_dis_kand_urit_nauk_120009_Kiiv_2017_277_c.

121. Каланча І. Г. Тенденції та динаміка застосування практики Європейського суду з прав людини під час кримінального провадження: статистичне та соціологічне дослідження. *Теорія і практика правознавства*, Вип. 2(18), 2020. С. 14 (1-17). URL: <https://doi.org/10.21564/2225-6555.2020.18.213676>.

122. Каланча І. Г. Термінологічне розмежування понять «електронний доказ», «цифровий доказ» і «доказ, що має електронну форму» в кримінальному процесі України. *Пріоритетні шляхи розвитку науки і освіти* : матеріали XV Міжнар. наук.-практ. конф. (м. Львів, 9–10 трав. 2025 р.). Львів : Львівський науковий форум, 2025. С. 195–197.

123. Каланча І. Г. Цифрова складова кримінального процесу України в науці та практиці: структурно-функціональний аналіз. *Сучасні виклики та актуальні*

проблеми судової реформи в Україні : матеріали VIII Міжнар. наук.-практ. конф. (м. Чернівці, 31 жовт. 2024 р.) / редкол. : О. В. Щербанюк та ін. Чернівці : 2024. С. 229–233.

124. Каланча І. Г. Шляхи формування сучасних практичних компетентностей у випускників правничих шкіл України. *Інноваційні рішення в сучасній науці, освіті та практиці* : матеріали I Міжнар. наук.-практ. інтернет-конф. (м. Київ, 17–18 листоп. 2020 р.) : у 2 ч. Київ : НТУ, 2020. Ч. 2. С. 209–212. URL: <http://vstup.ntu.edu.ua/conf-innov-part-2.pdf>.

125. Каланча І. Г., Гаркуша А. М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*. 2021. № 8. С. 336–339. URL: <https://doi.org/10.32782/2524-0374/2021-8/77>.

126. Каланча І. Г., Орлеан А. М. Адаптація системи кримінальної юстиції до цифровізації світу: роль навчального компоненту. *Наукові перспективи*. 2024. № 11 (53). С. 937–944. URL: [https://doi.org/10.52058/2708-7530-2024-11\(53\)-937-944](https://doi.org/10.52058/2708-7530-2024-11(53)-937-944).

127. Каланча І. Г., Стемковський Д. Б. Використання доказів, що мають електронну форму в кримінальному процесі України: судова практика. *Аналітично-порівняльне правознавство*. 2025. № 2. С. 1001–1008. URL: <https://doi.org/10.24144/2788-6018.2025.02.148>.

128. Каланча І. Г., Щербанюк О. В. Досудовий процес. Навчально-методичний посібник. Чернівці: Рута. Чернівецький національний університет імені Юрія Федьковича, 2020. 200 с.

129. Каланча І. Г., Юрчишин Ю. В. Забезпечення безпеки прокурора під час роботи з електронним сегментом кримінального провадження в Україні. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки*. 2024. Том 35 (74), № 6. С. 108–115. URL: <https://doi.org/10.32782/TNU-2707-0581/2024.6/19>.

130. Капліна О. В. Кримінальне процесуальне доказування та його суб'єкти. *Право України*. 2014. № 10. С. 136–147.

131. Капліна О. В. Правозастосовне тлумачення норм кримінально-процесуального права: Монографія. Х.: Право, 2008. 296 с.

132. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан ; за ред. О. Денькович, Г. Шмельцер. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL: <https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf>

133. Коваленко А. В. Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2018. Вип. 4. С. 237–245.

134. Коваленко А. В. Огляд комп'ютерних даних під час розслідування колабораційної діяльності: типові об'єкти та приклади з практики. *Війна в Україні: зроблені висновки та незасвоєні уроки* : зб. тез Міжнар. наук.-практ. конф. (м. Львів, 22–23 лют. 2024 р.). Львів : Львівський державний університет внутрішніх справ, 2024. С. 413–417.

135. Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Науковий вісник Херсонського державного університету. Серія: Юридичні науки*. 2023. Вип. 4. С. 53–58. DOI: 10.32999/ksu2307-8049/2023-4-9.

136. Коваленко А. В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2022. № 4. С. 226–236.

137. Коваленко В. В. Актуальні проблеми застосування науково-технічних засобів спеціалістами при провадженні слідчих дій : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2004. 16 с. URL: https://www.researchgate.net/profile/Volodymyr-Kovalenko-3/publication/395535420_Na_pravah_rukopisu/links/68c956ec4eef4b024b8bcbfa/Napravah-rukopisu.pdf.

138. Коваленко Є. Г. Теорія доказів у кримінальному процесі України : підручник. Київ : Юрінком Інтер, 2016. 632 с.

139. Ковальчук С. О. Вчення про речові докази у кримінальному процесі: теоретико-правові та практичні основи : дис. ... д-ра юрид. наук : 12.00.09. Одеса, 2018. 626 с.

140. Козицька О. Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2020. № 8. С. 418–421.

141. Козленко А. А. Належність та допустимість доказів у кримінальному провадженні : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2018. 19 с.

142. Колесник В. А. Використання положень цифрової криміналістики в оперативній та слідчій практиці. *Юридична наука: проблеми та шляхи їх вирішення. Тема року: Розвиток юридичної науки України в умовах воєнного стану* : зб. матеріалів І Міжнар. наук.-практ. конф. (м. Київ, 6 берез. 2025 р.). Київ : Приватний вищий навчальний заклад «Європейський університет», 2025. С. 88–92.

143. Колесник В. А. Криміналістичне забезпечення протидії терористичним загрозам критичній інфраструктурі. *Загальнодержавна система боротьби з тероризмом в умовах воєнного стану: стан, проблеми, шляхи удосконалення* : зб. матеріалів круглого столу (м. Київ, 31 жовт. 2024 р.). Київ : НАСБУ, 2024. С. 78–91.

144. Колесник В. А. Окремі напрями криміналістичного забезпечення боротьби з кіберзлочинами. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : матеріали Міжнар. наук.-практ. конф. (м. Київ, 20 груд. 2024 р.). Київ : КНДІСЕ, 2024.

145. Колесник В. А. Питання досудового розслідування злочинів проти інформаційної безпеки держави. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : матеріали IV Міжнар. наук.-практ. конф. (м. Київ, 16 груд. 2022 р.). Київ : Ун-тет «Україна», 2022.

146. Колесник В. А. Цифрова криміналістика та її місце в системі криміналістичних знань. *Актуальні питання криміналістики та судової експертизи* : матеріали міжвідом. наук.-практ. круглого столу (м. Київ, 21 листоп. 2024 р.). Київ : Нац. акад. внутр. справ, 2024. С. 40–44.

147. Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки, схвалений Указом Президента України від 11 травня 2023 р. № 273/2023. URL: <https://zakon.rada.gov.ua/laws/show/273/2023#Text>

148. Конвенція про кіберзлочинність від 23.11.2001 р., ратифікована Законом № 2824-IV від 07.09.2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575.

149. Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи : автореф. дис. ... канд. юрид. наук : 12.00.09. МВС України, Харк. нац. ун-т внутр. справ. Харків, 2017. 20 с. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/ae3bf4b6-9291-451f-bc4c-ccb5091a79e8/content>.

150. Котляревський О. І., Киценко Д. М. Комп'ютерна інформація як речовий доказ у кримінальній справі. Інформаційні технології та захист інформації : збірник наукових праць. Запоріжжя, 1998. № 2. С. 70–79.

151. Крет Г. Р. Міжнародні стандарти доказування у кримінальному процесі України: теоретико-правові та практичні основи : монографія. Калуш : Петраш К. Т., 2020. 452 с.

152. Криміналістика : підручник / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. ; за ред. проф. В. Ю. Шепітька. 4-е вид., перероб. і доп. Харків: Право, 2008. 464 с. URL: <https://law.sspu.edu.ua/files/documents/books/library/17/shepitko.pdf>.

153. Криміналістичне забезпечення збирання й використання електронних доказів у кримінальному провадженні : монографія / І. В. Гора, В. А. Колесник, О. С. Старенький, В. О. Ходанович, А. М. Черняк, Л. І. Щербина ; за заг. ред. В. А. Колесника. Київ : 7БЦ, 2025. 502 с.

154. Кримінальний кодекс України від 05.04.2001 р. № 2341-III (зі змін. та допов.). URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>.

155. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>.

156. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : колективна монографія / А. В. Гутник, А. Я. Хитра. Львів : ЛьвДУВС, 2022. 204 с.

157. Крицька І. О. Речові докази та цифрова інформація: поняття та співвідношення. *Часопис Київського університету права*. 2016. № 1. С. 301–305.

158. Крицька І. О. Речові докази у кримінальному провадженні : дис. ... канд. юрид. наук : 12.00.09. Національний юридичний університет імені Ярослава Мудрого. Харків, 2017. 249 с.

159. Кузубова Т. О. Правові засади інституту тимчасового доступу до речей та документів у кримінальному провадженні : дис. канд. юрид. наук : 12.00.09. Харків, 2019. 250 с.

160. Лисенко В. В. Проблеми отримання і використання у доказовому процесі інформації, що міститься у електронному вигляді на магнітних, оптичних чи інших носіях (за матеріалами діяльності податкової міліції). *Вісник прокуратури*. 2007. № 4. С. 61–69.

161. Литвинчук О. І. Електронні докази. Обшук. Частина 1 / О. І. Литвинчук, М. С. Сорока, І. В. Колесников та ін. Харків : Фактор, 2020. 80 с.

162. Лушпієнко В. М. Показання свідка як процесуальне джерело доказів у кримінальному процесі України : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ. нац. ун-т ім. Т. Шевченка. Київ, 2018. 20 с.

163. Любавіна В. П., Скляренко Г. В. Проведення комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2023. № 17. С. 36–40. URL: <https://journals.dpu.kyiv.ua/index.php/law/article/view/308/292>.

164. Макбрайд Д. Застосовні міжнародно-правові рамки та стандарти щодо доказів із відкритих та електронних джерел: Європейська конвенція з прав людини. Council of Europe : веб-сайт. URL: <https://rm.coe.int/coe-ukraine-open-uk/1680a6e571>.

165. Малахова О. В. Реалізація інституту сприяння захисту у кримінально-процесуальному доказуванні : автореф. дис. ... канд. юрид. наук : 12.00.09. Одеса,

2016. 20 с. URL: <https://dspace.onua.edu.ua/server/api/core/bitstreams/91d9f299-4aed-46b0-93a1-8a1c2bdfe24d/content>.

166. Матвеев В. Проблеми та виклики, пов'язані зі збором електронних доказів. 27.07.2023. Justtalk. URL: <https://justtalk.com.ua/post/problemi-ta-vikliki-povyazani-zi-zboromelektronnih-dokaziv>.

167. Метелев О. П. Гносеологічна і правова природи цифрових доказів у кримінальному процесі. *Правова позиція*. 2018. № 1 (20). С. 75–86.

168. Метелев О. П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2020. Вип. 60. С. 177–180.

169. Метелев О. П. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процесі. *Вісник кримінального судочинства*. 2019. № 3. С. 224–238.

170. Метелев О. П. Цифрові докази як окремий вид доказів у кримінальному процесі. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення*. Харків : Право, 2018. Вип. 10. С. 100–104.

171. Метелев О. П., Коваленко Є. В. До питання використання у кримінальному процесі цифрової інформації, отриманої під час контррозвідувальної та оперативно-розшукової діяльності. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 80(2). С. 177–182.

172. Мілімко Л. В., Жидовцев Я. В. Електронні докази в кримінальному судочинстві України. *Науковий вісник Ужгородського Національного Університету, Серія ПРАВО*. 2025. Вип. 88. Ч. 3. С. 302–308. URL: https://www.researchgate.net/publication/392347214_Electronic_evidence_in_criminal_proceedings_of_Ukraine.

173. Мовний коментар до Конституції України та інших нормативних актів / уклад. : Сергій Головатий, Світлана Сидоренко, Ірина Савченко ; комент. : Катерина Городенська, Лариса Колібаба, Валентина Фурса ; вступ. слово Павла

Гриценка ; за заг. ред. Павла Гриценка, Сергія Головатого; Конституц. Суд України, Пост. коміс. з питань правн. термінології ; Ін-т укр. мови НАН України. Харків : Право, 2025. 352 с.

174. Можливості використання додатка Google Earth Pro під час виявлення та розслідування кримінальних правопорушень. Застосування космічних і геоінформаційних технологій під час виявлення та розслідування кримінальних правопорушень : метод. рек. / авт. кол.: С. С. Чернявський, В. І. Присяжний, О. М. Стрільців, Д. І. Овсянюк та ін. ; за заг. ред. М. С. Цуцкірідзе. 2-ге вид., випр. і доповн. Київ : Нац. акад. внутр. справ, 2024. 93 с.

175. Музиченко О. В., Карандась М. В. Електронні докази як джерела доказів у межах кримінального провадження: судова практика та нормативне регулювання інших процесуальних кодексів України. *Київський часопис права*. 2022. № 2. С. 168–174. URL: <https://doi.org/10.32782/klj/2022.2.25>.

176. Мурадов В. В. Електронні докази: криміналістичний аспект використання. *Порівняльно-аналітичне право*. 2013. № 3-2. С. 316–318.

177. Нарійчук О.Д. Показання обвинуваченого як джерело доказів у кримінальному процесі України : дис. ... канд. юрид. наук : 12.00.09. Нац. акад. внутр. справ. Київ, 2012. 229 с.

178. Носов В. В., Овсянюк Д. І., Чіпуріна Г. А. Концептуальні засади вдосконалення навчання прокурорів, слідчих та оперативних працівників у сфері збирання електронних доказів, розслідування кіберзлочинів та суміжних напрямів. *Безпека у кіберсфері* : зб. матеріалів Міжнар. наук.-практ. конф. (м. Кам'янець-Подільський, 28 трав. 2025 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Нац. акад. правових наук України ; Організація з безпеки та співробітництва в Європі. Кам'янець-Подільський : ХНУВС, 2025. С. 171–173.

179. Овсянюк Д. І. Удосконалення навичок збору інформації з відкритих джерел (OSINT) в умовах воєнного стану в закладах вищої освіти зі специфічними умовами навчання, які здійснюють підготовку поліцейських. *Актуальні питання та перспективи розшукової роботи в діяльності підрозділів кримінальної поліції* : матеріали міжвідом. наук.-практ. круглого столу (м. Київ, 28 берез. 2024 р.) /

редкол.: В. В. Черней, С. Д. Гусарєв, С. С. Чернявський та ін. Київ : Нац. акад. внутр. справ, 2024. С. 102–105.

180. Овсянюк Д. І., Худенко Д. М. Використання підрозділами кримінального аналізу технологій розпізнавання облич та фенотипування ДНК в умовах воєнного стану. *Актуальні питання та перспективи використання оперативно-розшукових засобів у розкритті злочинів в умовах воєнного стану* : матеріали міжвідом. наук.-практ. конф. (м. Київ, 30 берез. 2023 р.) / редкол.: В. В. Черней, С. Д. Гусарєв, С. С. Чернявський та ін. Київ : Нац. акад. внутр. справ, 2023. С. 231–235.

181. Орлов Ю. Ю., Чернявський С. С. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ*. 2017. № 1 (13). С. 112–124.

182. Острійчук О. П. Показання як процесуальне джерело доказів у кримінальному провадженні : автореф. дис. ... канд. юрид. наук : 12.00.09. Донец. юрид. ін-т МВС України. Кривий Ріг, 2016. 18 с.

183. Пазюк А. В., Глинська Н. В. Міжнародно-правове регулювання використання відкритих джерел та електронних доказів у розслідуванні воєнних злочинів в контексті російсько-української війни. *Європейські перспективи*. 2024. № 3. С. 327–336.

184. Панченко Є. В., Овсянюк Д. І. Аналіз кластерів та адрес гаманців віртуальних активів (криптовалюти) для збору коштів на допомогу російській армії та іншим НЗФ. *Актуальні проблеми кібербезпеки в Україні в умовах воєнного стану* : матеріали міжвідом. наук.-практ. круглого столу (м. Київ, 25 квіт. 2024 р.) ; за заг. ред. В. А. Кудінова, К. В. Ярового. Київ : Нац. акад. внутр. справ, 2024. С. 108–113.

185. Пашковський М. І. Документування міжнародних злочинів неурядовими організаціями і використання отриманої цифрової інформації у кримінальних провадженнях за статтею 438 КК України. Альманах наукових праць фахівців НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України за результатами досліджень у 2022 р. / редкол.: В. С. Батиргарєєва, В. І.

Борисов, Д. П. Євтеєва та ін. ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, 2023. С. 70–80.

186. Пашковський М. І. Ланцюг зберігання доказів (chain of custody): процесуальна форма. *Інноваційна наука: пошук відповідей на виклики сучасності* : зб. наук. праць з матеріалами III Міжнар. наук. конф. (м. Могилів-Подільський, 6 груд. 2024 р.). Вінниця : ТОВ «УКРЛОГОС Груп, 2024. С. 157–161. URL: <https://archives.mcnd.org.ua/index.php/conference-proceeding/article/view/385/382>.

187. Пашковський М. І. Обставини, що мають значення для кримінального провадження та належність цифрових доказів з відкритих джерел. *Наукові перспективи*. 2024. № 10(52). С. 984–998. URL: https://www.researchgate.net/profile/Mykola-Pashkovskyi/publication/385728857_Obstavini_so_maut_znacenna_dla_kriminalnogo_provadzenna_ta_naleznist_cifrovih_dokaziv_z_vidkritih_dzerel/links/6777097500aa3770e0d1c99b.pdf.

188. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : автореф. дис. ... канд. юрид. наук: 12.00.09 / Харків. нац. ун-т внутр. справ. Харків, 2007 19 с.

189. Перцова-Тодорова Л. «Електронний доказ» під час обшуку. Підприємництво, господарство і право. 2020. № 6. С. 243–247.

190. Пиріг І. В. Теорія і практика використання спеціальних знань при розслідуванні розкрадань вантажів на залізничному транспорті : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ. нац. ун-т внутр. справ. Київ, 2006. 20 с.

191. Плєскач В. Л., Затонацька Т. Г. Інформаційні системи і технології на підприємствах : підручник. Київ : Знання, 2011. 718 с.

192. Погорецький М. А. Використання цифрових технологій у доказуванні та розслідуванні воєнних злочинів: виклики та перспективи. Актуальні питання криміналістики та судової експертизи: матеріали міжвідом. наук.-практ. круглого столу. (Київ, 21 листоп. 2024 р.). Київ : Нац. акад. внутр. справ, 2024. С. 431–437. URL: <https://elar.navs.edu.ua/handle/123456789/37824>

193. Погорецький М. А. Внесок професора М. М. Михеєнка у теорію кримінально-процесуальних доказів. *Проблеми кримінально-процесуального та цивільного процесуального права*: матер. Міжн. наук.-практ. конф., присвяч. пам'яті професорів кафедри правосуддя М. М. Михеєнка та М. Й. Штефана. Київ : ВГЛ “Обрії”, 2009. С. 28–31.

194. Погорецький М. А. Воєнний кримінальний процес: новели КПК та виклики правам людей. Кримінальне судочинство: сучасний стан та перспективи розвитку : матеріали Всеукр. наук.-практ. конф. (Київ, 2 трав. 2024 р.). Київ : Нац. акад. внутр. справ, 2024. С. 305–309 URL: <https://elar.navs.edu.ua/handle/123456789/37823>

195. Погорецький М. А. Докази у кримінальному процесі. *Вісник прокуратури*. 2003. № 2. С. 59–65.

196. Погорецький М. А. Докази у кримінальному процесі: проблемні питання. *Часопис Національного університету «Острозька академія». Серія «Право»*. 2011. № 1 (3): URL: <https://lj.oa.edu.ua/articles/2011/n1/11pmapppp.pdf>

197. Погорецький М. А. Доказування у кримінальному процесі: гносеологічні і правові проблеми. *Вісник Акад. правових наук України*. 2008. № 3. С. 266–275.

198. Погорецький М. А. Доктрина доказів XIX – поч. XXI ст. та її вплив на сучасну теорію доказів. *Вісник кримінального судочинства*. 2024. № 3–4. С. 32–44. DOI: <https://doi.org/10.17721/2413-5372.2024.3-4/53-85>. URL: <https://vkslaw.com.ua/index.php/journal/article/view/809/704>

199. Погорецький М. А. Допустимість доказів у кримінальному процесі та процесуальна доброчесність: доктрини і практика (порівняльно-правове дослідження). *Вісник кримінального судочинства*. 2025. № 1–2. С. 60–82. URL: <https://vkslaw.com.ua/index.php/journal/issue/view/37/1-2-2025-pdf>

200. Погорецький М. А. Еволюція доказів у кримінальному процесуальному законодавстві XIX століття та їх вплив на кримінальне процесуальне законодавство країн ЄС і України: порівняльно-правовий аналіз. *Вісник кримінального*

судочинства. 2024. № 1–2. С. 24–35. DOI: <https://doi.org/10.17721/2413-5372.2024.1-2/2024/30-50> URL: <https://vkslaw.com.ua/index.php/journal/article/view/767/677>

201. Погорецький М. А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів (проблемні питання). *Вісник кримінального судочинства*. 2023. № 3-4. С. 84-102. DOI: <https://doi.org/10.17721/2413-5372.2023.3-4/84-102>. URL: https://vkslaw.knu.ua/wp-content/uploads/2025/05/visnyk_krim_sud_3-4_23_v2_250425_avt2-84-102.pdf

202. Погорецький М. А. Нова концепція кримінального процесуального доказування. *Вісник кримінального судочинства України*. 2015. № 3. С. 63–79. URL: https://vkslaw.knu.ua/images/verstka/3_2015_Pogoretskyi.pdf

203. Погорецький М. А. Старенький О. С. Безпосередність дослідження доказів. Велика українська юридична енциклопедія: у 20 т. Харків: Право, 2016. Т.19: Кримінальний процес, судоустрій, прокуратура та адвокатура / редкол.: В. Т. Нор (голова) та ін.; Нац. акад. прав. наук. України ; Ін-т держави і права ім. В. М. Корецького НАН України ; Нац. юрид. ун-т ім. Ярослава Мудрого. 2020. С. 50-53.

204. Погорецький М. А. Сучасні концепції кримінального процесуального доказування. Сучасні тенденції розвитку криміналістики та кримінального процесу. Харків, 2017. С. 309-312. URL: https://univd.edu.ua/general/publishing/konf/08_11_2017/pdf/146.pdf

205. Погорецький М. А. Теорія доказів – методологічна основа оперативно-розшукового документування організованої злочинної діяльності. *Боротьба з організованою злочинністю і корупцією (теорія і практика): наук.-практ. журнал*. 2010. № 22. С. 175–185. URL: http://nbuv.gov.ua/UJRN/boz_2010_22_23.

206. Погорецький М. А. Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі: монографія. Харків: Арсіс ЛТД, 2007. 576 с.

207. Погорецький М. А., Лисаченко Є. І. Встановлення достовірності цифрових доказів Міжнародним кримінальним судом: окремі проблемні питання та шляхи їх вирішення. *Вісник кримінального судочинства*. 2023. № 1–2. С. 54–73.

DOI: <https://doi.org/10.17721/2413-5372.2023.1-2/54-73>.

URL:

<https://vkslaw.com.ua/index.php/journal/article/view/35>

208. Погорецький М. А., Лисаченко Є. І. Допустимість доказів у кримінальному процесуальному праві країн Європейського Союзу та його вплив на допустимість доказів у кримінальному судочинстві України. *Вісник кримінального судочинства*. 2022. № 3–4. С. 20–34. DOI: <https://doi.org/10.17721/2413-5372.2022.3-4/20-34> URL: <https://vkslaw.knu.ua/en/3-4-2022-actual-problems-of-criminal-justice/problems-of-the-criminal-process/admissibility-of-evidence-in-the-criminal-procedure-law-of-the-european-union-and-its-impact-on-criminal-justice-in-ukraine/>

209. Погорецький М. А., Сергєєва Д. Б. Тактика захисника: поняття, зміст та місце в системі криміналістичної тактики. *Вісник кримінального судочинства*. 2016. № 2. С. 113–123. URL: https://vkslaw.knu.ua/images/verstka/2_2016_Sergeeva.pdf

210. Погорецький М. Поняття, зміст та структура кримінального процесу: проблеми теорії та практики. *Право України*. 2013. С. 42-54.

211. Погорецький М. Теорія доказів як методологічна основа використання матеріалів оперативно-розшуковій діяльності у кримінальному процесі. Міжнародна поліцейська енциклопедія: у 10 т. / відп. ред. В. В. Коваленко, Є. В. Моїсєєв, В. Я. Тацій, Ю. С. Шемшученко. Київ : Атіка, 2010. Т. VI: Оперативно-розшукова діяльність поліції (міліції). С. 1011–1020.

212. Погорецький М. Теорія кримінального процесуального доказування: проблемні питання. *Право України*. 2014. № 10. С. 12-25. URL: https://pravoua.com.ua/uk/store/pravoukr/pravoukr_10_14/Pogoretskyi_10_14

213. Погорецький М., Шеломенцев В. Оперативно-рошукова діяльність у кіберпросторі. *Вісник прокуратури*. 2011. № 3. С. 58-63.

214. Положення про електронні освітні ресурси : наказ Міністерства освіти і науки; молоді та спорту України від 01.10.2012 р. № 1060. URL: <http://zakon2.rada.gov.ua/laws/show/z1695-12>.

215. Поляк Ю. П. Застосування технічних засобів при проведенні слідчих (розшукових), негласних слідчих (розшукових) дій та використання його

результатів під час досудового розслідування : дис. ... д-ра філософії : 081-Право. Львів : Львівський державний університет внутрішніх справ. 2022. 230 с.

216. Портал дистанційного навчання ТЦПУ. URL: <https://el.gp.gov.ua/moodle/>.

217. Порядок атестації та державної реєстрації методик проведення судових експертиз : Постанова Кабінету Міністрів України від 02.07.2008 р. № 595 (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/show/595-2008-%D0%BF#Text>.

218. Порядок ведення Реєстру методик проведення судових експертиз : наказ Міністерства юстиції України від 02.10.2008 р. № 1666/5 (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/show/z0924-08#Text>.

219. Пояснювальна записка до проекту Закону України «Про внесення змін до деяких законодавчих актів щодо забезпечення дотримання прав учасників кримінального провадження та інших осіб правоохоронними органами під час здійснення досудового розслідування». URL: <http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=62853&pf35401=438050>.

220. Правова інформація та комп'ютерні технології в юридичній діяльності: навч. посіб. / В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін. ; за заг. ред. В. Г. Іванова. 4-те вид., змін. і доп. Х. : Право, 2014. 240 с.

221. Про адвокатуру та адвокатську діяльність : Закон України від 05.07.2012 р. № 5076-VI. URL: <https://zakon.rada.gov.ua/laws/show/5076-17#Text>.

222. Про бухгалтерський облік та фінансову звітність в Україні : Закон України від 16.07.1999 р. № 996-XIV (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/show/996-14#Text>.

223. Про внесення змін до деяких нормативно-правових актів з питань судово-експертної діяльності : наказ Міністерства юстиції України від 21.06.2022 р. № 2578/5. URL: <https://zakon.rada.gov.ua/laws/show/z0687-22#Text>.

224. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон

України від 15.03.2022 р. № 2137-IX. URL: <https://zakon.rada.gov.ua/laws/show/2137-20#n35>.

225. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text>.

226. Про електронні комунікації : Закон України від 16.12.2020 р. № 1089-IX (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/show/1089-20#n771>.

227. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>.

228. Про електронну комерцію : Закон України від 3 верес. 2015 № 675-VIII. (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/show/675-19#Text>.

229. Про затвердження Інструкції про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол : наказ від 17.08.2020 р. № 613/380/93/228/414/510/2801/5. URL: <https://zakon.rada.gov.ua/laws/show/z0849-20#Text>.

230. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5.07.1994 р. № 80/94-ВР (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.

231. Про захист персональних даних Закон України від 1 червня 2010 року № 2297-VI (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.

232. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.

233. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

234. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 р. № 2824-IV. URL: <https://zakon.rada.gov.ua/laws/show/2824-15#Te>.

235. Про судову експертизу : Закон України від 25.02.1994 р. № 4038-XII (зі змін. і доп.). URL: <https://zakon.rada.gov.ua/laws/show/4038-12#Text>.

236. Про утворення територіального органу Національної поліції : Постанова Кабінету Міністрів України від 13.10.2015 р. № 83. URL: <https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF>.

237. Професор Ольга Шило. Творчий спадок / упоряд.: В. М. Трофименко, С. В. Давиденко, О. І. Марочкін. Харків : Право, 2023. 688 с.

238. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права, з прав людини та гуманітарного права / неофіц. пер. з англ. О. В. Зюзь. Нью-Йорк і Женева : Центр з прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. 119 с. URL: <https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf>.

239. Ратнова А. В. Електронний документ як джерело доказу у кримінальному провадженні. *Процесуальне та криміналістичне забезпечення досудового розслідування* : зб. тез наук.-практ. семінару (м. Львів, 1 груд. 2017 р.). Львів : ЛьвДУВС, 2017. С. 90–94.

240. Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. ... д-ра філософії : 081-Право. Львів : Львівський державний університет внутрішніх справ, 2021. 248 с.

241. Рішення МКС у справі «Прокурор проти Ахмада Аль-Факі Аль-Махді (Prosecutor v. Ahmad Al Faqi Al Mahdi). Заява ICC-01/12-01/15 від 27.09.2016. URL: https://www.icccpi.int/sites/default/files/CourtRecords/CR2016_07244.PDF.

242. Рішення МКС у справі «Прокурор проти Махмуда Мустафи Бусайф аль-Верфаллі» (Prosecutor v. Mahmoud al-Werfalli). Заява ICC-01/11-01/17 від 04.07.2018. URL:

https://www.icccpi.int/sites/default/files/CourtRecords/CR2018_03552.PDF.

243. Самойленко О. А. Виявлення та розслідування кіберзлочинів : навч.-метод. посіб. Одеса, 2020. 112 с.
244. Самойлов С. В. Фіксації вмісту інтернет ресурсів під час кримінального провадження: порівняльний аналіз слідчого експерименту та огляду. *Пріоритетні шляхи розвитку науки і освіти* : матеріали XIV Міжнар. наук.-практ. конф. (м. Львів, 29–30 січ. 2025 р.). Львів : Львівський науковий форум, 2025. С. 68–70.
245. Сергєєва Д. Б. Допустимість доказів в теорії та КПК 2012 року. Вісник кримінального судочинства. 2015. № 3. С. 80-87. URL: <https://vkslaw.com.ua/index.php/journal/article/view/708>.
246. Сергєєва Д. Б. Належність доказів за новим КПК України. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2013. № 3 (спец. вип.). С. 234-239. URL: [http://nbuv.gov.ua/UJRN/boz_2013_3\(spets](http://nbuv.gov.ua/UJRN/boz_2013_3(spets)
247. Сергєєва Д. Б. Поняття та сутність достовірності доказу як його властивості. Юрист України. 2014. № 1. С. 89–95. URL: http://nbuv.gov.ua/UJRN/uy_2014_1_14.
248. Сіренко О. В. Електронні докази у кримінальному провадженні. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2019. Вип. 14. С. 208–214.
249. Скрипник А. В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні : дис. ... д-ра філософії : 081-Право. Харків : Національний юридичний університет імені Ярослава Мудрого, 2021. 369 с.
250. Смалъ І. А. Теоретичні засади формування та практика застосування електронних доказів у кримінальному процесі. дис. ... д-ра філос. за спец. (081 – Право). Пенітенціарна академія України, 2025. 329 с. URL: https://pau.edu.ua/one-time-specialized-scientific-councils/df7_2025/.
251. Смирнов В. А. Допустимість як критерій оцінки доказів у кримінальному провадженні : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2021. 24 с.

252. Сольонова О. О. Показання потерпілого як джерело доказів у кримінальному провадженні : автореф. дис. ... канд. юрид. наук : 12.00.09. Нац. акад. внутр. справ. Київ, 2018. 20 с.

253. Старенький О. С. Кримінальні процесуальні гарантії захисника як суб'єкта доказування у досудовому розслідуванні: теорія та практика : монографія. Київ. нац. ун-т ім. Т. Шевченка; За заг. ред. М. А. Погорецький. Київ : Алерта : Правова Єдність, 2016. 334 с.

254. Стахівський С. М. Кримінально-процесуальні засоби доказування : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2005. 32 с.

255. Степанов О. С. Належність та допустимість доказів в кримінальному процесі України : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2007. 16 с.

256. Стоянов М. М. Властивості доказів у кримінальному процесі України : автореф. дис. ... канд. юрид. наук : 12.00.09. Нац. ун.-т "Одеська юридична академія". Одеса, 2010. 20 с.

257. Стефанів Н. Матеріальний носій – лише спосіб збереження інформації, який має значення тільки тоді, коли Е-документ виступає речовим доказом. Інформагентство «ADVOKAT POST». 02.11.2021. URL: <https://advokatpost.com/materialnyj-nosij-lyshe-sposib-zberezhennia-informatsii-iakyj-maie-znachennia-tilky-todi-koly-e-dokument-vystupaie-rechovym-dokazom-suddia-stefaniv/>.

258. Столітній А. В. Електронне кримінальне провадження на досудовому розслідуванні : дис. ... д-ра. юрид. наук : 12.00.09 / Національна академія прокуратури України, Дніпропетровський державний університет внутрішніх справ. Дніпро, 2018. 648 с.

259. Столітній А. В. Електронний висновок експерта в кримінальному провадженні. *Криміналістика і судова експертиза*. 2019. Вип. 64. С. 102-111. URL: http://nbuv.gov.ua/UJRN/krise_2019_64_11.

260. Столітній А. В., Каланча І. Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. 2019. Вип. 146. С. 179–191. URL: <https://doi.org/10.21564/2414-990x.146.171218>.

261. Стратегія кібербезпеки України, схвалена рішенням Ради національної безпеки і оборони України від 14 травня 2021 року та уведена в дію Указом Президента України від 26 серпня 2021 р. № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>.

262. Стратегія розвитку прокуратури на 2025-2028 роки, затвердженої наказом Генерального прокурора № 322 від 8 жовтня 2025 р. URL: https://old.gp.gov.ua/ua/file_downloader.html?_m=fslib&_t=fsfile&_c=download&file_id=274671.

263. Стратегія розвитку системи правосуддя та конституційного судочинства на 2021-2023 р.р., затверджена Указом Президента України від 11 червня 2021 р. № 231/2021. URL: <https://zakon.rada.gov.ua/laws/show/231/2021#Text>.

264. Судові експертизи в процесуальному праві України : навч. посіб. / за заг. ред. О. Г. Рувіна. Київ : Видавництво Ліра-К, 2019. 424 с.

265. Сурмін Ю. П. Кейс-метод: становлення та розвиток в Україні. Вісник Національної академії державного управління при Президентові України. 2015. № 2. С. 19–28.

266. Теплицький Б. Б. Завдання, об'єкти й питання комп'ютерно-технічної судової експертизи. *Науковий вісник Національної академії внутрішніх справ*. 2018. № 3. С. 303–315.

267. Теплицький Б. Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. ... канд. юрид. наук : спец. 12.00.09. Нац. акад. внутр. справ. Київ, 2021. 268 с.

268. Тertiшник В. М. Теорія доказів : підручник. Київ : Алерта, 2015. 394 с.

269. Тетерятник Г. К., Виходець Ю. О. Теоретичні та праксеологічні аспекти фіксування та використання у кримінальному процесуальному доказуванні інформації з інтернет-джерел. *Юридичний науковий електронний журнал*. 2022. № 10. С. 772–776. URL: <https://doi.org/10.32782/2524-0374/2022-10/194>.

270. Тичина Д. М., Антошук А. О., Перцев Р. В. Криміналістичне забезпечення використання безпілотного літального апарату (дрону у досудовому

розслідуванні. *Науковий вісник ужгородського національного університету. Серія ПРАВО*. 2023. Вип. 78, ч. 2. С. 291–297. URL: <https://doi.org/10.24144/2307-3322.2023.78.2.46>.

271. Тичина Д. М., Перцев Р. В., Антощук А. О. Іноземний досвід використання тепловізора на безпілотному літальному апараті (дроні) при проведенні огляду місця події. *Право і суспільство*. 2024. № 4. С. 316–322. URL: <https://doi.org/10.32842/2078-3736/2024.4.43>.

272. Тітко І. А. Алібі // Велика українська енциклопедія. URL: <https://vue.gov.ua/Алібі>.

273. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Видавництво «Юридика», 2024. 180 с.

274. Тютюнник В. В. Інститут допустимості доказів як гарантія ухвалення законного та обґрунтованого вироку суду : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2016. 20 с.

275. Удалова Л. Д. Теорія та практика отримання вербальної інформації у кримінальному процесі України: Монографія. К . : Вид. Паливода А. В., 2005. 324 с.

276. Удалова Л. Д. Теоретичні засади отримання вербальної інформації у кримінальному процесі України : дис... д-ра юрид. наук: 12.00.09. Київський національний ун-т внутрішніх справ. Київ, 2007. 433 с. 412.

277. Фоміна Т. Г., Рачинський О. О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник Харківського національного університету внутрішніх справ*. 2023. № 3 (102), ч. 2. С. 207–220. URL: <https://doi.org/10.32631/v.2023.3.43>.

278. Хижняк Є. С. Віртуальні сліди: поняття та ознаки. *Правове життя сучасної України* : у 2 т. : матер. Міжнар. наук.-практ. конф. (м. Одеса, 17 трав. 2019 р.) / відп. ред. Г. О. Ульянова. Одеса : ВД «Гельветика», 2019. Т. 2. С. 422–425. URL: <https://hdl.handle.net/11300/21544>.

279. Хижняк Є. С. До питання визначення поняття «віртуальні сліди». *Наука та суспільне життя України в епоху глобальних викликів людства у цифрову*

еру (з нагоди 30-річчя проголошення незалежності України та 25-річчя прийняття Конституції України) : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 21 трав. 2021 р.) / за заг. ред. С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2021. Т. 2. С. 377–379. URL: <https://hdl.handle.net/11300/15070>.

280. Хижняк Є. С. Особливості ідентифікації особи злочинця за допомогою IP-адреси. *Правове життя сучасної України* : у 3 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.) / відп. ред. М. Р. Аракелян. Одеса : Гельветика, 2020. Т. 3. С. 353–356. URL: <https://hdl.handle.net/11300/13345>.

281. Хом'яченко С. І., Часова Т. О. Використання електронних доказів у кримінальному процесі. *Право. Людина. Довкілля: науково-практичний журнал*. 2020. 11 (2). С. 175–181.

282. Цехан Д. М. Правові аспекти використання цифрової інформації як доказу у кримінальному судочинстві. *Процесуальні, тактичні та психологічні проблеми, тенденції та перспективи вдосконалення досудового слідства* : матеріали між- нар. наук.-практ.конф. (Одеса, 30 травня 2008 р.). Одеса. 2008. С. 206–209.

283. Цехан Д. М. Цифрові докази: поняття, особливості та місце в системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2013. № 5. С. 256–260.

284. Цехан Д. М., Мурашко А. С. Використання соціальних медіа для вирішення ідентифікаційних завдань під час виявлення та розслідування злочинів, пов'язаних із державною зрадою. *Юридичний науковий електронний журнал : електронне наукове фахове видання*. 2024. Вип. 2. С. 481–483. URL: <https://dspace.onua.edu.ua/server/api/core/bitstreams/b91efc8f-ab3e-4850-92f6-071e4f58de0a/content>.

285. Чекотило В. І. Залучення експерта до кримінального провадження : автореф. дис. ... канд. юрид. наук : 12.00.09. МВС України, Харк. нац. ун-т внутр. справ. Харків, 2015. 22 с. URL: <https://dspace.univd.edu.ua/items/18f0df2c-048e-4e98-be15-7b50cd5eb93b>.

286. Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування : монографія. Київ : Хай-Тек Прес. 2010. 624 с.

287. Чигрина Г. Л. Джерела доказів у кримінальних справах про ухилення від сплати податків, зборів, інших обов'язкових платежів : автореф. дис. ... канд. юрид. наук : 12.00.09 / Національний університет внутрішніх справ. Київ, 2004. 21 с.

288. Чупрікова І. Л. Допустимість доказів у світлі нового Кримінального процесуального кодексу: дис. ... канд. юрид. наук : 12.00.09. Одеса, 2016. 191 с.

289. Шаповаленко Є. В. Деякі аспекти встановлення місцезнаходження особи, яка знаходиться у розшуку, за допомогою фіксування та збереження цифрової інформації з відкритих джерел. *Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності* : тези V Всеукр. наук.-практ. конф. (м. Хмельницький, 25 лют. 2022 р.). Хмельницький : Вид-во НАДПСУ, 2022. С. 1008–1010.

290. Шведова О. В. Комплексне криміналістичне дослідження документів, виконаних за допомогою комп'ютерних технологій : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2006. 19 с.

291. Шевчук П. В., Каланча І. Г. Кримінальний процес : навчально-методичний посібник. Чернівці, 2024. 184 с.

292. Шепітько В. Ю., Авдєєва Г. К. Проблеми розроблення інноваційних засад техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції. *Питання боротьби зі злочинністю*. 2014. Вип. 27. С. 156–165. URL: http://nbuv.gov.ua/UJRN/Pbzz_2014_27_17.

293. Шепітько В., Авдєєва Г. Використання сучасних досягнень науки і техніки у боротьбі зі злочинністю: здобутки та перспективи діяльності наукової лабораторії. *Вісник Національної академії правових наук України*. 2013. № 2. С. 308–313. URL: http://nbuv.gov.ua/UJRN/vapny_2013_2_38.

294. Шумило М. Є. Поняття доказів у кримінальному процесі. *Вісник кримінального судочинства*. 2015. № 3. С. 95–104. URL: https://vkslaw.knu.ua/images/verstka/3_2015_Shumilo.pdf

295. Шумило М. Є. Юридична конструкція доказів у кримінальному провадженні. *Вісник кримінального судочинства*. 2018. № 1. С. 59-67. URL: http://nbuv.gov.ua/UJRN/vkc_2018_1_8

296. Щербаковський М. Г. Теоретико-методологічні та праксеологічні засади судових експертиз у кримінальному процесі : автореф. дис. ... д-ра юрид. наук : 12.00.09. Харків, 2016. 40 с.

297. Щур Н. О., Покотило О. А. Основи криптології : навч. посіб. Житомир : Державний університет «Житомирська політехніка», 2021. 120 с.

298. Юрчишин В. Д. Висновок експерта як джерело доказів у кримінальному процесі України : дис. ... канд. юрид. наук : 12.00.09. Прикарпатський національний університет імені Василя Стефаника. Івано-Франківськ, 2007. 227 с. URL: <https://uacademic.info/ua/document/0407U001213>.

299. Яремчук В. О. Залучення спеціаліста до проведення слідчих дій (організація і тактика) : автореф. дис. ... канд. юрид. наук : 12.00.09. Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2014. 20 с. URL: <https://dspace.nlu.edu.ua/handle/123456789/5897>.

300. 100 Stat. 1848 – Electronic Communications Privacy Act of 1986. URL: <https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1848>.

301. 18 U.S. Code Chapter 121 Part I – Stored Wire And Electronic Communications And Transactional Records Access. URL: <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>.

302. ACPO Good Practice Guide for Digital Evidence. URL: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.

303. Act on Communications Interception for Criminal Investigation. Act No. 137 of August 18, 1999. (Last Version : Act No. 63 of 2019). Japanese Law Translation Database System. 2025. Ministry of Justice, Japan. URL: <https://www.japaneselawtranslation.go.jp/en/laws/view/3857/en>.

304. Act on Electronic Signatures and Certification Business. Act No. 102 of May 31, 2000. (Last Version : Act No. 10 of 2000). Japanese Law Translation Database System. 2025. Ministry of Justice, Japan. URL: <https://www.japaneselawtranslation.go.jp/en/laws/view/3821/en>.

305. Act on promotion of the digitalization of the criminal justice process. Act No. 9942, Jan. 25, 2010 (Amended by Act No. 12844, Nov. 19, 2014; Act No. 14839, Jul. 26, 2017; Act No. 18653, Dec. 28, 2021). Korea Law Translation Center. URL: https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=60123&key=9&type=part.

306. Act on the use of electronic documents in criminal justice procedures. Act No. 18485, Oct. 19, 2021. Korea Law Translation Center. URL: https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=60861&key=9&type=part.

307. Agbedanu P. R., Wang P., Nortey R. N. Odartey L. K. Forensics in the Cloud: A Literature Analysis and Classification. In 2019 5th International Conference on Big Data Computing and Communications (BIGCOM). 2019. P. 124–132. URL: <https://doi.org/10.1109/BIGCOM.2019.00027>.

308. Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime. URL: https://assets.publishing.service.gov.uk/media/5d9b01dfe5274a5a243406e7/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

309. Al-Dhaqm A., Ikuesan R.A., Kebande V.R., Razak S.A., Grispos G., Choo K.-K.R., Al-Rimy B.A.S., Alsewari A.A. Digital Forensics Subdomains: The State of the Art and Future Directions. *IEEE* 2021. Vol. 9. P. 152476–152502. URL: <https://doi.org/10.1109/ACCESS.2021.3124262>.

310. Alex J. Paper-based vs. electronic evidence tracking. URL: <https://pmievidencetracker.com/2020/02/17/paper-based-vs-electronic-evidence-tracking/>.

311. Ali M., Ismail A., Elgohary H., Darwish S., Mesbah S. A procedure for tracing chain of custody in digital image forensics: A paradigm based on grey hash and blockchain. *Symmetry*. 2022. Vol. 14. No. 2. P. 334. URL: <https://doi.org/10.3390/sym14020334>.

312. Almulla S., Iraqi Y., Jones A. Cloud forensics: A research perspective. In 9th International Conference on Innovations in Information Technology. 2013. P. 66–71.

313. Antwort der Bundesregierung auf die Kleine Anfrage der Martina Renner, Dr. André Hahn, Gökay Akbulut, Clara Bünger, Anke Domscheit-Berg, Nicole Gohlke, Jan Korte, Ina Latendorf, Cornelia Möhring, Petra Pau, Sören Pellmann, Dr. Petra Sitte, Kathrin Vogler und der Gruppe Die Linke. Drucksache 20/12944. URL: <https://dserver.bundestag.de/btd/20/131/2013130.pdf>.

314. Arrêté du 25 mai 2016 fixant le cadre national de la formation et les modalités conduisant à la délivrance du diplôme national de doctorat. URL: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000032587086>.

315. Azərbaycan Respublikasının Cinayət-Prosesual Məcəlləsi: 14 iyul 2000-cu il tarixli 907-IQ nömrəli Azərbaycan Respublikasının Qanunu (Azərbaycan Respublikasının qanunvericilik toplusu, 2000-ci il, № 8 (II kitab), maddə 585) ilə təsdiq edilmişdir (dəyişikliklər və əlavələr nəzərə alınıb) / Azərbaycan Respublikası Ədliyyə Nazirliyi nomativ hüquqi aktların vahid internet elektron bazası. URL: <http://www.e-qanun.az/code/14>.

316. Bai V. S., Sudha T. A Systematic Literature Review on Cloud Forensics in Cloud Environment. *International Journal of Intelligent Systems and Applications in Engineering*. 2023. Vol. 11. P. 565–578.

317. Baudžiamojo proceso kodeksas, Lietuvos Respublikos, patvirtintas 2002 m. kovo 14 d. įstatymu Nr. IX-785 (Galiojanti suvestinė redakcija: 2020-01-01). URL: <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/XgMEabiNkE>.

318. Berkeley Protocol on Digital Open Source Investigations. A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. New York and Geneva,

2022. 102 p. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf.

319. Best Practice Manual for the Forensic Examination of Digital Technology ENFSI-BPM-FIT-01 Version 01 – November 2015. 65 p. URL: https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf.

320. Boneh D., Shoup V. A Graduate Course in Applied Cryptography. 2023. 1130 p. URL: https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_6.pdf.

321. Bonomi S., Casini M., Ciccotelli C. B-coc: A blockchain-based chain of custody for evidences management in digital forensics. URL: <https://doi.org/10.48550/arXiv.1807.10359>.

322. Bruce I. Forced biometric authentication – on a recent amendment in the Norwegian Code of Criminal Procedure. *Digital Evidence and Electronic Signature Law Review*, № 14. 2017. URL: <https://journals.sas.ac.uk/deeslr/article/view/2429?utm>.

323. BS EN ISO/IEC 27037:2016. Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: <https://knowledge.bsigroup.com/products/information-technology-security-techniques-guidelines-for-identification-collection-acquisition-and-preservation-of-digital-evidence>.

324. Bundesgericht Tribunal fédéral. 7B_576/2024. Urteil vom 20. März 2025. URL: https://search.bger.ch/ext/eurospider/live/de/php/aza/http/index.php?highlight_docid=aza%3A%2F%2F20-03-2025-7B_576-2024&lang=de&type=show_document&zoom=.

325. Burman M., Smith O., Brooks-Hay O., Brunger Y. Digital Communications as Evidence in Sexual Offence Applications to the Criminal Cases Review Commission. Glasgow : Scottish Centre for Crime and Justice Research. 2025. 36 p. URL: https://www.sccjr.ac.uk/wp-content/uploads/2025/06/CCRC-Final-Report_April-2025.pdf.

326. Cabinet Resolution No. (28) of 2023 on the Executive Regulations of Federal Decree-Law No. (46) of 2021 on Electronic Transactions and Trust Services. Issued Date

31 Mar 2023. Effective Date 13 Jul 2023. Official Gazette Date 14 Apr 2023. Official Gazette No 749. URL: <https://uaelegislation.gov.ae/en/legislations/2199/download>.

327. Case of AFFAIRE BERSHEDA ET RYBOLOVLEV c. MONACO. (Requêtes nos 36559/19 et 36570/19). European Court of Human Rights. HUDOC. URL: [https://hudoc.echr.coe.int/spa#{%22itemid%22:\[%22001-234090%22\]}](https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-234090%22]}).

328. Case of Ahmet Yildirim v. Turkey (Application no. 3111/10) : Judgment of ECHR of 18 December 2012 European Court of Human Rights. HUDOC. URL: <http://hudoc.echr.coe.int/fre?i=001-126893>.

329. Case of Cengiz and Others v. Turkey (Applications nos. 48226/10 and 14027/11) : Judgment of ECHR of 1 December 2015. European Court of Human Rights. HUDOC. URL: <http://hudoc.echr.coe.int/eng?i=001-159188>.

330. Case of Contrada v. Italy (no. 4) (Application no. 2507/19) : Judgment of the ECtHR of 23 May 2024 European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/ukr?i=001-233733>.

331. Case of Copland v. the United Kingdom (Application no. 62617/00): Judgment European Court of Human Rights, 3 April 2007. European Court of Human Rights. HUDOC. URL: <http://hudoc.echr.coe.int/eng?i=001-79996>.

332. Case of Georgia v. Russia (II) (Application no. 38263/08) : Judgment of the ECtHR of 21 Jan. 2021. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-207757>.

333. Case of Golder v. the United Kingdom (Application no. 4451/70) : Judgment of the ECtHR of 21 Febr. 1975 European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/ukr?i=001-57496>.

334. Case of Golovan v. Ukraine (Application no. 41716/06) : Judgment of the ECtHR of 05 Oct. 2022. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/ukr?i=001-112021>.

335. Case of Klass and others v. Germany (Application no. 5029/71) : Judgment of the ECtHR of 6 Sept. 1978 European Court of Human Rights. HUDOC. URL: <http://hudoc.echr.coe.int/eng?i=001-57510>.

336. Case of Malone v. the United Kingdom (Application no. 8691/79) : Judgment of the ECtHR of 26 Apr. 1985. European Court of Human Rights. HUDOC. URL: <http://hudoc.echr.coe.int/eng?i=001-57532>.

337. Case of Petri Sallinen and Others v. Finland (Application № 50882/99) : Judgment European Court of Human Rights, 27 September 2005. European Court of Human Rights. HUDOC.. URL: <http://hudoc.echr.coe.int/eng?i=001-70283>.

338. Case of Plechlo v. Slovakia (Application no. 18593/19) : Judgment of the ECtHR of 26 Oct. 2023. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/ukr?i=001-228383>.

339. Case of Reznik v Ukraine (Application No. 31175/14) : Judgment of ECtHR, 23 Jan. 2025. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-240192>.

340. Case of Saber v. Norway (Application no. 459/18) : Judgment 17 Dec. 2020 : Judgment of the ECtHR of 17 Dec. 2020. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-206519>.

341. Case of Särgava v. Estonia (Application no. 698/19) : Judgment of the ECtHR of 16 Nov. 2021. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-213208>.

342. Case of Sérvulo & Associados - Sociedade de Advogados, RL and others v. Portugal (Application no. 27013/10) : Judgment of the ECtHR of 3 Sept. 2015. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/ukr?i=001-156519>.

343. Case of Ukrkava, TOV v. Ukraine (Application No. 10233/20) : Judgment of ECtHR, 06 Febr. 2025. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/ukr?i=001-241576>.

344. Case of Volokhy v. Ukraine (Application no. 23543/02) : Judgment of the ECtHR of 2 Nov. 2006. European Court of Human Rights. HUDOC. URL: <http://hudoc.echr.coe.int/eng?i=001-77837>.

345. Case of Wieser and Bicos Beteiligungen GmbH v. Austria (Application no. 74336/01) : Judgment of the ECtHR of 16 Oct. 2007. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/eng?i=001-82711>.

346. Case of Yuditskaya and others v. Russia (Application no. 5678/06) : Judgment of the ECtHR of 12 Febr. 2015. European Court of Human Rights. HUDOC. URL: <https://hudoc.echr.coe.int/ukr?i=001-151037>.

347. Casey E., Brenner S.W., Koops B.-J. et al. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd Edition. Elsevier, 2011. 807 p. URL: <https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf>.

348. Casino F., Pina C., Lopez-Aguilar P., Batista E., Solanas A., Patsakis C. SoK: Cross-border criminal investigations and digital evidence. Journal of Cybersecurity. 2022. Vol. 8(1), tyac014. URL: <https://doi.org/10.1093/cybsec/tyac014>.

349. Chen C. T., Cheng K. Y., Li, S. Y. Can Email Be Evidence for Adultery in Criminal Law Cases? A Philosophical and Legal Explication of the Court's Evaluation of Evidence through Inner Conviction. International Journal of Cyber Society and Education. Pages 1-20, Vol. 2, No. 1, June 2009. URL: <https://philarchive.org/archive/CHECEB?utm>.

350. Christopher L. T. Brown Computer Evidence: Collection And Preservation, Second Edition. Boston, 2010. 518 p.

351. Cinar B., Bharadiya J. P. Cloud computing forensics; Challenges and future perspectives: A review. Asian Journal of Research in Computer Science. 2023. Vol. 16(1). P. 1-14. <https://doi.org/10.9734/ajrcos/2023/v16i1330>.

352. CIR1H nr 9343 af 30/03/2022. Justitsministeriet. Offentliggørelsesdato 31/03/2022. Accession C20220934309. Entydig dokumentidentifikation AA013043. Dato for førstegangsendlæggelse 31/03/2022. Dato for seneste indlæggelse 31/03/2022. Dokumenttype Cirkulære (1 sp). Dokumentets rangering C. Forskriftens nummer 9343. År for udstedelse 2022. Dato for underskrift 30/03/2022. Offentliggjort i (publiceringsmedie) Retsinformation. Administrerende myndighed Rigsadvokaten. Ressortministeriets journalnummer CMS VB 9051. URL: <https://www.retsinformation.dk/eli/retsinfo/2022/9343>.

353. Clarifying Lawful Overseas Use of Data Act, Pub L No 115-141, div V, 132 Stat 348 (2018). URL: <https://www.justice.gov/criminal/media/999391/dl?inline>.

354. CMS Law, ‘SMS, emails et messages vocaux: les nouveaux moyens de preuve’ (CMS, 23 June 2016). URL: <https://cms.law/fr/fra/publication/sms-emails-et-messages-vocaux-les-nouveaux-moyens-de-preuve>.

355. Code de procédure pénale. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/.

356. Code de procédure pénale. Version consolidée applicable au 04/08/2025. Journal officiel du Grand-Duché de Luxembourg. URL: https://legilux.public.lu/eli/etat/leg/code/procedure_penale.

357. Code of Criminal Procedure (Part I and Part II). Act No. 131 of July 10, 1948. (Last Version : Act No. 36 of 2006). Japanese Law Translation Database System. 2025. Ministry of Justice, Japan. URL: <https://www.japaneselawtranslation.go.jp/en/laws/view/2056/en>.

358. Code of Judicial Procedure (Act No. 4/1734 of January 1, 1734, as amended up to Act No. 732 of June 6, 2015), Finland. URL: <https://www.wipo.int/wipolex/en/legislation/details/17980>.

359. Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System. Issue 4. October 2017. URL: https://assets.publishing.service.gov.uk/media/5a81cdd940f0b62305b90e5a/100_-_2017_10_09_-_The_Codes_of_Practice_and_Conduct_-_Issue_4_final_web_web_pdf__2_.pdf.

360. Codul de procedură penală al Republicii Moldova din 14.03.2003 Nr. 122 (cu modificări și completări de la 19.03.2019). URL: <http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=350171>.

361. Coercive Measures Act (806/2011; amendments up to 182/2024 included). Ministry of Justice, Finland. URL: <https://www.finlex.fi/api/media/statute-foreign-language-translation/688064/mainPdf/main.pdf>.

362. Cohen M., Garfinkel S., Schatz B. Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic

workflow. *Digital investigation*. 2009. Vol. 6. P. S57–S68. URL: <https://doi.org/10.1016/j.diin.2009.06.010>.

363. Cosic J., Bača M., A framework to (im)prove chain of custody in digital investigation process. In *Proceedings of the 21st Central European Conference on Information and Intelligent System*. 2010.

364. Cosic J., Bača M., Do we have full control over integrity in digital evidence life cycle? In *32nd International Conference on Information Technology Interfaces (ITI)*. 2010. P. 429-434.

365. Cosic J., Cosic Z. Chain of custody and life cycle of digital evidence. *Computer technology and application*. 2012. № 3 (2). P. 127. URL: https://www.researchgate.net/publication/279175015_Chain_of_custody_and_life_cycle_of_digital_evidence.

366. Council of Europe (CE) TRT/CE-224P2CC/001. Second Additional Protocol to the Convention on Cybercrime on enhanced Co-operation and Disclosure of Electronic Evidence. URL: <https://www.wipo.int/wipolex/en/text/586521>.

367. Council of Europe HELP course on Cybercrime and Electronic Evidence was launched. 24 April 2024. Council of Europe. URL: <https://www.coe.int/en/web/kyiv/-/council-of-europe-help-course-on-cybercrime-and-electronic-evidence-was-launched>.

368. Crime of Preparation of Acts of Terrorism and Other Organized Crimes. The Ministry of Justice. Japan. URL: https://www.moj.go.jp/EN/keiji1/keiji12_00143.htmlhttps://www.moj.go.jp/EN/keiji1/keiji12_00143.html.

369. Criminal Code. R.S.C., 1985, c. C-46. Government of Canada. URL: <https://laws-lois.justice.gc.ca/eng/acts/c-46/section-487.0195.html>.

370. Criminal Procedure Act. Act No. 341, Sep. 23, 1954 (Amended by ... Act No. 18799, Feb. 3, 2022). Korea Law Translation Center. URL: https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=60539&key=9&type=part.

371. Criminal Procedure Code 2010. Current version as at 02 Dec 2025. Attorney-General's Chambers of Singapore. URL: <https://sso.agc.gov.sg/Act/ETA2010>; <https://sso.agc.gov.sg/Act/CPC2010>.

372. Criminal Procedure Law. By China Law Translate. URL: <https://www.chinalawtranslate.com/en/criminal-procedure-law-2018/>.

373. Daniele M. Digital Evidence gathering from service providers: a worrying paradigm shift in international cooperation. *Brazilian Journal of Criminal Procedure*. 2019. Vol. 5. No. 3. P. 1277–1296. URL: <https://doi.org/10.22197/rbdpp.v5i3.288>.

374. Décret n° 2006-580 du 23 mai 2006 portant publication de la Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001 (1). URL: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000788820>.

375. Digital Evidence in Germany: Legal Foundations, Collection, and Admissibility in Court. URL: <https://www.ferner-alsdorf.com/digital-evidence-in-germany-legal-foundations-collection-and-admissibility-in-court/>.

376. Digital Evidence Policy Guide 0830PG Part 01 (Final). URL: <https://vault.fbi.gov/digital-evidence-policy-guide-0830pg/Digital%20Evidence%20Policy%20Guide%200830PG%20Part%2001%20%28Final%29/view>.

377. Digital Forensics. URL: <https://www.nist.gov/itl/ssd/digital-forensics?utm>.

378. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32023L1544>.

379. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. URL: <https://eur-lex.europa.eu/eli/dir/2006/24/oj/eng>.

380. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0041>.

381. Du J., Ding L., Chen, G. Research on the Rules of Electronic Evidence in Chinese Criminal Proceedings. *International Journal of Digital Crime and Forensics*. Volume 12. Issue 3. July-September 2020. p.p. 111-121. URL: [https://pdfs.semanticscholar.org/78c5/a268e70834b3cc0446669e92a12f586ade24.pdf?u](https://pdfs.semanticscholar.org/78c5/a268e70834b3cc0446669e92a12f586ade24.pdf?utm)tm.

382. Dulskyi O., Leliuk T., Luhovyi V., Melnyk V., Morgun I. International cooperation when collecting evidence in the investigation of transnational organised crime: Challenges and opportunities. *Revista Amazonia Investiga*. 2023. Vol. 12(70). P. 88-101. URL: <https://doi.org/10.34069/ai/2023.70.10.8>.

383. Dykstra J., Sherman A. T. Understanding Issues in cloud forensics: Two hypothetical case studies. *Journal of Network Forensics*. 2011. Vol. 3. P. 19–31.

384. EDPB-EDPS Joint Response on the US Cloud Act. URL: https://www.edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-response-us-cloud-act_en.

385. Electronic Communications and Transactions Act, 2002. No. 25 of 2002. Government Gazette. Republic Of South Africa. Vol. 446. Cape Town. 2 August 2002. No. 23708. The Presidency. No. 1046. 2 August 2002. URL: https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf?utm.

386. Electronic evidence – a basic guide for First Responders. 26 p. URL: [https://syntheticdrugs.unodc.org/uploads/syntheticdrugs/res/library/cybercrime_html/El](https://syntheticdrugs.unodc.org/uploads/syntheticdrugs/res/library/cybercrime_html/Elctronic_Evidence_A_Basic_Guide_for_First_Responders_ENISA.pdf)ectronic_Evidence_A_Basic_Guide_for_First_Responders_ENISA.pdf.

387. Electronic Evidence and Electronic Signatures: 5th Edition. Ed. by Stephen Mason and Daniel Seng. 2021. 604 p. URL: <https://library.oapen.org/handle/20.500.12657/55755>.

388. Electronic evidence guide as basic guide for police officers, prosecutors and judges/ Version 2.1. Cybercrime division. Directorate General of Human Rights and Rule of Law. Strasbourg. 2020. 200 p.

389. El-Kady R. M. Handling E-evidence in Egyptian and comparative legislation: A comparative analytical study. *Arab Journal of Forensic Sciences and Forensic Medicine*. 2023. Vol. 5(2). P. 191-222. URL: <https://doi.org/10.26735/WGZY6322>.

390. EN ISO/IEC 27037:2016. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: <https://standards.iteh.ai/catalog/standards/cen/ff19a638-8301-45c0-8bb4-92965b0296ab/en-iso-iec-27037-2016?srsId=AfmBOoqTFp55oMiyXaFcyzQeU0bseH5gR7V1uzp6GtwYfZ1FquMyq2Wx>.

391. Erik Sinander The Swedish Supreme Court on the Taking of Digital Evidence in International Cases. 27 June 2022. URL: <https://eapil.org/2022/06/27/the-swedish-supreme-court-on-the-taking-of-digital-evidence-in-international-cases/?utm>.

392. Esler W Brian. Lorraine V Markel: Unnecessarily Raising The Standard For Admissibility Of Electronic Evidence. *Digital Evidence and Electronic Signature Law Review*. URL: <https://sas-space.sas.ac.uk/5473/1/1803-2471-1-SM.pdf>.

393. e-Trials. Supreme Court of Korea. URL: <https://eng.scourt.go.kr/eng/judiciary/eCourt/eTrials.jsp>.

394. ETSI TS 119 312 V1.4.3 (2023-08). Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. Official edition. 2023. URL: https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.03_60/ts_119312v010403p.pdf.

395. Euromed Digital Evidence Manual. Practical Guide for Requesting Electronic Evidence from Service Providers. URL: <https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/manual-on-digital-evidence%204-4-19.pdf?utm>.

396. Evaluating digital open source imagery: A guide for judges and fact-finders. 2024. URL: <https://www.trueproject.co.uk/osguide>.

397. Evidence Act 1893. (Section 116A(5)1). Evidence (Computer Output). Regulations 1996. Current version as at 02 Dec 2025. Attorney-General's Chambers of Singapore. URL: <https://sso.agc.gov.sg/SL/EA1893-RG1>.

398. Evidence Act 1893. Current version as at 02 Dec 2025. Attorney-General's Chambers of Singapore. URL: <https://sso.agc.gov.sg/Act/EA1893>.

399. Evidence Act 1950 (Revised 1971). Malaysian Legislation. URL: https://www.commonlii.org/my/legis/consol_act/ea19501971155/.

400. EVS-EN ISO/IEC 27037:2016. Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence. URKL URL: <https://www.evs.ee/en/evs-en-iso-iec-27037-2016>.

401. Ewald U. Digital Forensics vs. Due Process: Conflicting Standards or Complementary Approaches? In Proceedings of the Third Central European Cybersecurity Conference, CECC 2019. 2019. Association for Computing Machinery, New York, NY, USA. URL: <https://doi.org/10.1145/3360664.3362697>.

402. Federal Decree by Law No. (35) of 2022 Promulgating the Law of Evidence in Civil and Commercial Transactions. Issued Date 03 Oct 2022. Effective Date 02 Jan 2023. Official Gazette Date 10 Oct 2022. Official Gazette No 737. URL: <https://uaelegislation.gov.ae/en/legislations/1612>.

403. Federal Decree by Law No. (38) of 2022, Promulgating the Criminal Procedures Law. Issued Date 03 Oct 2022. Effective Date 01 Mar 2023. Official Gazette Date 10 Oct 2022. Official Gazette No 737. URL: <https://uaelegislation.gov.ae/en/legislations/1609>.

404. Federal Decree by Law No. (46) of 2021 on Electronic Transactions and Trust Services. Issued Date 20 Sep 2021. Effective Date 02 Jan 2022. Official Gazette Date 26 Sep 2021. Official Gazette No 712 (ملحق1). URL: <https://uaelegislation.gov.ae/en/legislations/1539>.

405. Federal Law No. (10) of 2019 on Regulating Judicial Relations Among the Judicial, Federal and Local Authorities. FED LAW No. 10 of 2019. Gazette No. 669. UAE Official Gazette. URL: <https://uaelegislation.gov.ae/en/legislations/1431/download?utm>.

406. Federal Rules of Evidence. URL: <https://www.law.cornell.edu/rules/fre>.

407. Féral, ‘La jurisprudence de la Cour de cassation en matière de preuve électronique’ (Féral, 2018). URL: <https://feral.law/archives/la-jurisprudence-de-la-cour-de-cassation-en-matiere-de-preuve-electronique>.

408. France. Cybercrime policies/strategies. URL: <https://www.coe.int/en/web/octopus/-/france>.

409. Fredesvinda I. The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime - Results of a European Study. *Journal of Digital Forensic Practice*. 2007. 1:4. P. 1. DOI:10.1080/15567280701418049.

410. Galushko A., Ochi M. (Eds.) Collecting Cyber Evidence During Ongoing Hybrid Warfare: OSINT and Civilian-led Documentation of Core International Crimes. Apeldoorn-Antwerp.Maklu. 2025. 297 p.

411. German Code of Criminal Procedure (Strafprozeßordnung – StPO). URL: https://www.gesetze-im-internet.de/englisch_stpo/.

412. German court finds hacked EncroChat phone evidence inadmissible. URL: <https://www.computerweekly.com/news/366617630/German-court-finds-hacked-EncroChat-phone-evidence-inadmissible>.

413. Giova G. Improving chain of custody in forensic investigation of electronic digital systems. *International Journal of Computer Science and Network Security*. 2011. Vol. 11. No. 1. Pp. 1–9. URL: https://www.researchgate.net/publication/267400650_Improving_Chain_of_Custody_in_Forensic_Investigation_of_Electronic_Digital_Systems.

414. Grispos G., Storer T., Glisson W. Calm before the storm: The challenges of cloud computing in digital forensics. *International Journal of Digital Crime and Forensics*. 2012. Vol. 4 (2). P. 28–48.

415. Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence / Council of Europe, European Court of Human Rights. ECtHR, 2024. 180 p. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng.

416. Guidelines for digital forensics first responders. Best practices for search and seizure of electronic and digital evidence. March 2021. INTERPOL. 55 p. URL: https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf.

417. Gupta G., Husain A. Digital evidence in police investigation: A comparative analysis of challenges faced in India, the UK and the United States. *Journal of Victimology and Victim Justice*. 2023. Vol. 6(2). URL: <https://doi.org/10.1177/25166069231184977>.

418. Handys und Laptops von Verdächtigen – Wie die Daten-Flut Polizei und Justiz überfordert Autorenprofilbild von Denis Fengler. Redakteur WELT/WELT AM SONNTAG Hamburg. Veröffentlicht am 05.08.2024. URL: <https://www.welt.de/regionales/hamburg/article252811554/Strafverfolgung-Handys-und-Laptops-von-Verdaechtigen-Wie-die-Daten-Flut-Polizei-und-Justiz-ueberfordert.html>.

419. Hettige K. H. A., Fernando M. S. D. A survey on issues in cloud forensics with an experiment on time consumption. *International Journal of Advanced and Applied Sciences*. 2022. Vol. 9(3). P. 19-30. URL: <https://doi.org/10.21833/ijaas.2022.03.003>.

420. Hinweisportal und Integrierte Untersuchungs- und Auswerteumgebung (IUA). URL: <https://mik.brandenburg.de/mik/de/themen/brandenburg-paket/hinweisportal-iaa/#>.

421. Hloviuk I., Zavtur V., Zinkovskyy I., Fedorov I. Te use of video and audio recordings provided by victims of domestic violence as evidence. *Social & Legal Studios*. 2024. № 7(1). P. 145–154. URL: <https://doi.org/10.32518/sals1.2024.145>.

422. Hodge Gail M. Best Practices for Digital Archiving an Information Life Cycle Approach. 2000. URL: <http://www.dlib.org/dlib/january00/01hodge.html>.

423. How to comply with both the GDPR and the CLOUD Act. Walter Delacruz, Matthias Artzt. URL: <https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act>.

424. International cooperation against cybercrime. URL: https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime/international-cooperation-against-cybercrime_en.

425. INTERPOL I-24/7 Global Police Communication System. URL: <https://interpollawfirm.com/blog/interpol-i247-data-removal/>.

426. Investigatory Powers Act 2016. URL: <https://www.legislation.gov.uk/ukpga/2016/25>.

427. IOCE Principles and definition, IOCE Conference, 1999. IOCE, Guidelines for best practice in the forensic examination of digital technology, 2002. Guidelines For Best Practice In The Forensic Examination Of Digital Technology, IOCE 2002 Digital Evidence Standards Working Group.

428. ISO/IEC 10118-3:2018(en). IT Security techniques - Hash-functions – Part 3: Dedicated hash-functions. Official edition. 2018. URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:10118:-3:ed-4:v1:en>.

429. ISO/IEC 27037:2012(en). Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27037:ed-1:v1:en>.

430. IT platform for exchange of electronic evidence between judicial authorities. URL: <https://ec.europa.eu/futurium/en/egovernment4eu/action-21-it-platform-exchange-electronic-evidence-between-judicial-authorities.html>.

431. IT und Technik beim BKA. URL: https://www.karriere.bka.de/Karriereportal/DE/Jobs/BerufeBeimBKA/Cluster_ItUndTechnik/itUndTechnik_node.html.

432. IT-Forensik: Spurensuche in Bits und Bytes. URL: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/IT-Forensik/it_forensik_node.html.

433. Jack R. LORRAINE and, Beverly Mack, Plaintiffs, v. MARKEL AMERICAN INSURANCE COMPANY, Defendants Civil Action No. PWG–06–1893 United States District Court, D. Maryland. May 04, 2007. URL: https://app.minerva26.com/case_law/17344-lorraine-v-markel-am-ins-co.

434. Joint US-EU Statement on Electronic Evidence Sharing Negotiations. Thursday, September 26, 2019. URL: <https://www.justice.gov/archives/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations>.

435. Kalancha I., Bozhyk V., Muzychenko O., Vatsiyk V. Digital evidence in comparative criminal procedure: international experience and the practice of judicial review. TPM – Testing, Psychometrics, Methodology in Applied Psychology. 2025. Vol. 32, No. S2. P. 34-46. URL: <https://tpmap.org/submission/index.php/tpm/article/view/150/34>.

436. Koops E. J. Cybercrime legislation in the Netherlands. in J H M van Erp & L P W van Vliet (eds), Netherlands Reports to the Eighteenth International Congress on Comparative Law. Intersentia, Antwerp, 2010, pp. 595-633. URL: <https://repository.tilburguniversity.edu/bitstreams/3351c56f-2441-4bd5-b531-7356edf39ba6/download>.

437. Kozii V., Kalancha I., Vlasova H., Orlean A. Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies. *IDP. Internet, Law an Politics Journal*. 2025. №. 42. P. 1–13. URL: <https://raco.cat/index.php/IDP/article/view/429924/526486>.

438. Kriminaalmenetluse seadustik: Seadus Eesti Vabariigi vastu võetud 12.02.2003, avaldamine RT I 2003, 27, 166 (muudatused ja täiendused on olemas) // Riigi Teataja võrguväljaande veebilehele. URL: <https://www.riigiteataja.ee/akt/119032019033>.

439. Kriminālprocesa likums. Latvijas Republikas. Likums Saeimā pieņemts 21.04.2005 (ar grozījumiem). URL: <https://likumi.lv/ta/id/107820>.

440. Kumari N., Mohapatra A.K. A Novel Framework For Multi Source Based Cloud Forensic. In 2022 6th International Conference on Computing Methodologies and Communication (ICCMC). 2022. Pp. 1–7. URL: <https://doi.org/10.1109/ICCMC53470.2022.9753849>.

441. Lasagni G. Bartoli L. The Handling of Digital Evidence in Italy. Digital Forensic Evidence: Towards Common European Standards in Antifraud Administrative and Criminal Investigations. 2021. p.p. 87-121 URL:

https://www.researchgate.net/publication/361092881_The_Handling_of_Digital_Evidence_in_Italy?utm.

442. Law of Criminal Procedure. Ministry of Justice. Kingdom of Saud Arabia. URL: <https://www.moj.gov.sa/Documents/Regulations/pdf/En/08.pdf>.

443. LBK nr 1835 af 15/09/2021. Justitsministeriet. Retsplejeloven. Offentliggørelsesdato 24/09/2021. Accession 20210183529. Entydig dokumentidentifikation AA012548. Dato for førstegangsindlæggelse 24/09/2021. Dato for seneste indlæggelse 24/09/2021. Dokumenttype Lovbekendtgørelse. Dokumentets rangering A. Forskriftens nummer 1835. År for udstedelse 2021. Dato for underskrift 15/09/2021. Offentliggjort i (publiceringsmedie) Lovtidende A. Ressortministeriets journalnummer Justitsmin., j.nr. 2021-4000-0187. URL: <https://www.retsinformation.dk/eli/lta/2021/1835>.

444. Lee C.-L. E-Justice in Taiwan: The Derivative Inquiries from Constitutional Perspectives in the Digital Age. *Ritsumeikan Law Review*. No. 40, 2022. p.p. 55-67. URL: <https://www.ritsumei.ac.jp/acd/cg/law/lex/rlr40/006Chien-Liang%20LEE.pdf?utm>.

445. Legalspace, 'La valeur juridique de l'email' (Legalspace, 12 April 2019). URL: <https://www.legalspace.com/dematerialisation/valeur-juridique-email>.

446. Li W., Wu J., Cao J., Chen N., Zhang Q., Buyya R. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. *Journal of Cloud Computing*. 2021. Vol. 10. URL: <https://doi.org/10.1186/s13677-021-00247-5>.

447. Lög um meðferð sakamála. 2008 nr. 88 12. Júní. Íslensk lög 1. september 2025. Útgáfa 156b. URL: <https://www.althingi.is/lagas/nuna/2008088.html>.

448. Loi du 27 juin 2018 adaptant la procédure pénale aux besoins liés à la menace terroriste et portant modification. *Journal officiel du Grand-Duché de Luxembourg*. URL: <https://legilux.public.lu/eli/etat/leg/loi/2018/06/27/a559/jo>.

449. Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et, portant modification des articles 88-2 et 88-4 du Code

d'instruction criminelle Journal officiel du Grand-Duché de Luxembourg. URL: <https://legilux.public.lu/eli/etat/leg/loi/2005/05/30/n4/jo>.

450. Losavio M., Seigfried-Spellar K. C., Sloan J. J. Why digital forensics is not a profession and how it can become one. *Criminal Justice Studies*. 2016. Issue 29(2). P. 143–162. URL: <https://doi.org/10.1080/1478601X.2016.1170281>.

451. Lucien L. Challenges of Trustworthy of Digital Evidence and Its Chain of Custody on Cloud Computing Environment: A Systematic Review. In *Proceedings of the 26th International Conference on Enterprise Information Systems*. 2024. Vol. 2: ICEIS, SciTePress. P. 241. URL: <https://doi.org/10.5220/0012702800003690>.

452. Lukic-Radovic M., Manojlovic-Nedeljkovic M. Effectiveness of the joint investigation team as an instrument for gathering and exchange of evidence in cross-border investigations. *Zbornik Radova Pravnog Fakulteta Nis*. 2023. Vol. 62(100). P. 93–124. URL: <https://doi.org/10.5937/zrpfno-46661>.

453. Martini B., Choo K. K. R. An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*. 2012. Vol. 9(2). P. 71–80. URL: <https://doi.org/10.1016/j.diin.2012.07.001>.

454. Mason S. *International Electronic Evidence*. London : British Institute of International and Comparative Law, 2008. 1002 p.

455. Mason S., Seng D. *Electronic Evidence: 4th Edition*. 2017. URL: <https://doi.org/10.14296/9781911507079>.

456. Mesarak M., Podrouzek J., Gavornik A. On defence of “ethification” of law: How ethics may improve compliance with the EU digital laws. *Computer Law and Security Review*. 2023. Vol. 50. P. 105852. URL: <https://doi.org/10.1016Zj.clsr.2023.105852>.

457. Miller C. M. A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy*. 2023. Vol. 6. P. 100296. URL: <https://doi.org/10.1016/j.fsisyn.2022.100296>.

458. Montasari R., Hill R. Next-Generation Digital Forensics: Challenges and Future Paradigms. In *2019 IEEE 12th International Conference on Global Security*,

Safety and Sustainability (ICGS3). London, UK, 2019. Pp. 205-212. URL: <https://doi.org/10.1109/ICGS3.2019.8688020>.

459. Morioka E., Sharbaf M. Cloud Computing: Digital Forensic Solutions. In 2015 12th International Conference on Information Technology – New Generations. Las Vegas, NV, USA, 2015. Pp. 589-594. URL: <https://doi.org/10.1109/ITNG.2015.99>.

460. Murachov R. Features of the organisation of interaction between the international criminal court and law enforcement structures of Ukraine regarding the investigation of crimes. *Analytical and Comparative Jurisprudence*. 2023. Vol. 6. P. 692-696. URL: <https://doi.org/10.24144/2788-6018.2023.06.119>.

461. Nakamura M. Remote Access Investigation in Japan. *Japanese Journal of Global Informatics*. Vol. 1, March 2021. p.p. 105-115. URL: https://chuo-u.repo.nii.ac.jp/record/12941/files/2435-855X_1_105-116.pdf.

462. Nath S., Summers K., Baek J., Ahn G. J. Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics. In *Proceedings – 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, TPS-ISA 2024*. Institute of Electrical and Electronics Engineers Inc., 2024. P. 13. <https://doi.org/10.1109/TPS-ISA62245.2024.00012>.

463. New regulation simplifies the exchange of digital evidence in criminal cases within Europe. 09-01-2024. URL: <https://www.government.nl/latest/news/2024/01/09/new-regulation-simplifies-the-exchange-of-digital-evidence-in-criminal-cases-within-europe?utm>.

464. NIST Policy on Hash Functions. NIST Computer Security Resource Center. URL: <https://csrc.nist.gov/Projects/Hash-Functions/NIST-Policy-on-Hash-Functions>.

465. Nosál J. Crime in the Digital Age: A New Frontier. In Berghofer, J., Futter, A., Häusler, C., Hoell, M., Nosál, J. (eds) *The Implications of Emerging Technologies in the Euro-Atlantic Space*. Palgrave Macmillan, Cham, 2023. URL: https://doi.org/10.1007/978-3-031-24673-9_11.

466. Okmi M., Por L. Y., Ang T. F., Al-Hussein W., Ku C. S. A systematic review of mobile phone data in crime applications: A coherent taxonomy based on data types

and analysis perspectives, challenges, and future research directions. *Sensors*. 2023. Vol. 29(9). P. 4350. URL: <https://doi.org/10.3390/s23094350>.

467. Onlinedurchsuchung und Quellen-TKÜ in der Strafprozessordnung – Neuordnung der tiefen technischen Eingriffsmaßnahmen in der StPO seit dem 24.8.2017. von OStA Dieter Kochheim. URL: <https://kripoz.de/2018/03/01/onlinedurchsuchung-und-quellen-tkue-in-der-strafprozessordnung-neuordnung-der-tiefen-technischen-eingriffsmassnahmen-in-der-stpo-seit-dem-24-8-2017/>.

468. Ordonnance n° 2016-1636 du 1er décembre 2016 relative à la décision d'enquête européenne en matière pénale. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000033511653>.

469. Ovsianiuk D., Okushko A., Panchenko Ye. Methodology of detection and forensic features of investigation of crimes involving virtual assets: A comparative analysis of international practices. *Scientific Journal of the National Academy of Internal Affairs*. 2025. Vol. 30, No. 2. P. 119–137. URL: <https://doi.org/10.63341/naia-herald/2.2025.119>.

470. Patreliuk D., Svoboda I., Kalancha I., Filashkin V., Kachmar B. Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations. *Pakistan Journal of Life and Social Sciences*. 2024. Vol. 22(2). P. 4811–4820. URL: <https://doi.org/10.57239/PJLSS-2024-22.2.00356>.

471. Perault M., Salgado R. Untapping the Full Potential of CLOUD Act Agreements. Posted on June 13, 2024. URL: <https://www.crossborderdataforum.org/untapping-the-full-potential-of-cloud-act-agreements/>.

472. Personal information protection act. Expand Act No. 16930, Feb. 4, 2020. Korean Legislation Research Institute. URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG.

473. Police Act(872/2011; amendments up to 1168/2013 included). Ministry of the Interior, Finland. URL: <https://www.finlex.fi/api/media/statute-foreign-language-translation/688066/mainPdf/main.pdf>.

474. Police and Criminal Evidence Act 1984. URL: <https://www.legislation.gov.uk/ukpga/1984/60/contents>.
475. Prakash V., Williams A., Garg L., Barik P., Dhanaraj R.K. Cloud-Based Framework for Performing Digital Forensic Investigations. *International Journal of Wireless Information Networks*. 2022. Vol. 29. P. 419–441. URL: <https://doi.org/10.1007/s10776-022-00560-z>.
476. Procedural manuals for the evidentiary law. Decision of The Minister of Justice NO (921). Publish Date 28.10.2022. Kingdom of Saud Arabia. URL: <https://laws.moj.gov.sa/en/legislation/ZNMI0PpA1fSRgK60lVLGEw>.
477. Procedural Manuals For The Evidentiary Law. Release Date 12/10/2022. Classification Judiciary. Statute Type Other (أدلة). Publish Date 28/10/2022. Statute Status Active. Statute Release Tool Decision of The Minister of Justice No (921). URL: <https://qanoniah.com/en/File/MyB5xjq4Zdoj8lp7k8va2P0AD-PROCEDURAL-MANUALS-FOR-THE-EVIDENTIARY-LAW>.
478. Promulgating the Cybercrime Prevention Law. Law No. (14) of 2014. Ministry of Justice State of Qatar. URL: <https://www.almeezan.qa/EnglishLaws/142014.pdf>.
479. Protection of communications secrets act. Expand Act No. 4650, Dec. 27, 1993. Korean Legislation Research Institute. URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=7235&lang=ENG.
480. Published Complete Listing. Scientific Working Group on Digital Evidence (SWGDE). URL: <https://www.swgde.org/documents-old/published-complete-listing-old/>.
481. Purnaye P., Kulkarni, V. A Comprehensive Study of Cloud Forensics. *Archives of Computational Methods in Engineering*. 2022. Vol. 29. P. 33–46. URL: <https://doi.org/10.1007/s11831-021-09575-w>.
482. R. v. Fearon, 2014 SCC 77, [2014] 3 S.C.R. 621. Date: 20141211. Docket: 35298. Supreme Court of Canada. URL: <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/14502/index.do>.

483. R. v. Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212. Date: 20140613. Docket: 34644. Supreme Court of Canada. URL: <https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/14233/index.do>.

484. Radhakrishna G. Section 90A Evidence Act 1950 of Malaysia: A time for review. In *Proceedings at the 5th. Annual International Conference on Law Regulation and Public Policy*. 2016, May. Vol. 30, p. 31. URL: https://www.researchgate.net/profile/Gita-Radhakrishna/publication/313673126_Section_90A_Evidence_Act_1950_of_Malaysia_Time_to_Review/data/58a28469a6fdccf5e9711345/GR-s-90A.pdf?origin=publication_list&utm_source.

485. Rasjid Z.E., Soewito B., Witjaksono G., Abdurahman E. Framework for establishing confidence level of digital evidence admissibility. *ICIC Express Letters*. 2019. Vol. 13. P. 663–672. URL: <https://doi.org/10.24507/icicel.13.08.663>.

486. Rättegångsbalk (1942:740). SFS nr: 1942:740. Departement/myndighet: Justitiedepartementet DÅ. Utfärdad: 1942-07-18. Ändrad: t.o.m. SFS 2025:860. URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/rattegangsbalk-1942740_sfs-1942-740/.

487. Regarding Promulgating the Criminal Procedure Code. Law no. (23) for 2004. Legislations in Qatar. URL: <https://www.almeezan.qa/LawPage.aspx?ID=3971&language=en>.

488. Regelungen zur präventiven und strafprozessualen (Quellen-) Telekommunikationsüberwachung und zur strafprozessualen Online-Durchsuchung halten verfassungsrechtlicher Überprüfung weitgehend Stand. Beschluss vom 24. Juni 2025 - 1 BvR 180/23/. Beschluss vom 24. Juni 2025 – 1 BvR 2466/19. URL: <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2025/bvg25-069.html>.

489. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

(General Data Protection Regulation) (Text with EEA relevance). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>.

490. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1543>.

491. Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R1025&utm>.

492. Reilly D., Wren C., Berry T. Cloud computing : Pros and cons for computer forensic investigations. *International Journal Multimedia and Image Processing*. 2011. Vol. 1 (1). P. 26–34.

493. Rojszczak M. CLOUD act agreements from an EU perspective. *Computer Law and Security Review*. 2020. Vol. 38. P. 105442. URL: <https://doi.org/10.1016/j.clsr.2020.105442>.

494. Rule 901. Authenticating or Identifying Evidence. URL: https://www.law.cornell.edu/rules/fre/rule_901; Rule 902. Evidence That Is Self-Authenticating. URL: https://www.law.cornell.edu/rules/fre/rule_902.

495. Rusman G., D'orio E., Popova E., Kipouras P. Features of the application of digital technology in criminal proceedings of the BRICS countries. *BRICS Law Journal*. 2023. Vol. 10(1). P. 35-58. URL: <https://doi.org/10.21684/2412-2343-2023-10-1-35-58>.

496. Schweizerische Strafprozessordnung (Strafprozessordnung, StPO) vom 5. Oktober 2007 (Stand am 1. April 2025). URL: <https://www.fedlex.admin.ch/eli/cc/2010/267/de>.

497. Secure Information Exchange Network Application (SIENA). Ensuring the secure exchange of sensitive and restricted information. URL: <https://www.europol.europa.eu/how-we-work/services-support/information-exchange/secure-information-exchange-network-application-siena>.

498. Service-public.fr, Preuve d'un fait ou d'un acte juridique (21 October 2019). URL: <https://www.service-public.fr/particuliers/vosdroits/F1800>.

499. Sharma P., Kumar M., Sharma H. Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: *An evaluation. Multimedia Tools and Applications*. 2023. Vol. 82(12). P. 18117-18150. URL: <https://doi.org/10.1007/s11042-022-13808-w>.

500. Sheldon John B. Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly*. 2011. Vol. 5. No. 2. P. 98. URL: <http://www.jstor.org/stable/26270559>.

501. Simou S., Kalloniatis C., Gritzalis S., Katos V. A framework for designing cloud forensic-enabled services (CFeS). *Requirements Engineering*. 2019. Vol. 24. P. 403–430. URL: <https://doi.org/10.1007/s00766-018-0289-y>.

502. SIST EN ISO/IEC 27037:2017. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: <https://standards.iteh.ai/catalog/standards/sist/cb1db2f0-c590-4fb6-8e01-43a1bcc5cf62/sist-en-iso-iec-27037-2017>.

503. Sree R.S., Raja K. A Review on Forensic Investigation Analysis in Cloud Computing Environments. In 2022 1st International Conf. *On Computational Science and Technology (ICCST)*. 2022. P. 1067–1074. URL: <https://doi.org/10.1109/ICCST55948.2022.10040384>.

504. Standard Operating Procedures for the Collection, Analysis and Presentation of Electronic Evidence / Cybercrime Programme Office of the Council of Europe (CPROC). EU : CoE, 2019. 39 p. URL: <https://rm.coe.int/3692-sop-electronicevidence/168097d7cb>.

505. Stanfield A. R The authentication of electronic evidence. PhD thesis. Queensland University of Technology. Brisbane, 2016. 268 p.

506. Stoykova R., Franke K. Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations. *Forensic Science International: Digital Investigation*. 2023. Vol. 45. P. 301554. URL: <https://doi.org/10.1016/j.fsidi.2023.301554>.

507. Sulisdyanoro D., Marzuki M. I. Identification of Whatsapp digital evidence on Android smartphones using the Android backup APK (application package Kit) downgrade method. *Journal of Integrated and Advanced Engineering (JIAE)*. 2023. Vol. 3(1). P. 7-22. URL: <https://doi.org/10.51662/jiae.v3i1.70>.

508. Supreme Court of the United States. No. 17–2united States, Petitioner V. Microsoft Corporation on Writ of Certiorari to the United States Court Ofappeals for the Second Circuit. April 17, 2018. URL: https://www.supremecourt.gov/opinions/17pdf/17-2_1824.pdf.

509. Supreme Court of the United States. Riley V. California. Certiorari to the Court of Appeal of California, Fourth Appellate District, Division One. No. 13–132. Argued April 29, 2014—Decided June 25, 2014. URL: <https://supreme.justia.com/cases/federal/us/573/13-132/case.pdf>.

510. SWGDE position on the use of MD5 and SHA1 hash algorithms in digital and multimedia forensics. URL: <https://www.swgde.org/wp-content/uploads/2023/09/2019-09-29-SWGDE-Position-on-the-Use-of-MD5-and.pdf>.

511. Syed S., Anu V. Digital Evidence Data Collection: Cloud Challenges. In 2021 *IEEE International Conference on Big Data (Big Data)*. 2021. P. 6032–6034. URL: <https://doi.org/10.1109/BigData52589.2021.9672014>.

512. Thakkar P., Patel D., Hirpara I., Jagani J., Patel S., Shah M. and Kshirsagar A. A Comprehensive review on computer vision and fuzzy logic in forensic science application. *Annals of Data Science*. 2023. Vol. 10. P. 761–785. URL: <https://doi.org/10.1007/s40745-022-00408-6>.

513. The Budapest Convention on Cybercrime, Council of Europe, Budapest, 23.11.2001. URL: <https://rm.coe.int/1680081561>.

514. The Cloud Act Is Not a Tool for Theft of Trade Secrets Justin Hemmings, Nathan Swire, April 23, 2019, 8:00 AM. URL: <https://www.lawfaremedia.org/article/cloud-act-not-tool-theft-trade-secrets>.

515. The Criminal Procedure Act. Act of 22 May 1981 No. 25. With subsequent amendments, the latest made by Act of 21 June 2013 No. 84. Ministry of Justice and Public security. DET KONGELIGE JUSTIS – OG BEREDSKAPSDEPARTEMENT. URL: https://legislationline.org/sites/default/files/documents/30/Norway_Criminal_Procedure_Act_1981_am2013_en.pdf.

516. The Handbook of Forensic Services provides guidance and procedures for safe and efficient methods of collecting, preserving, packaging, and shipping evidence and describes the forensic examinations performed by the FBI's Laboratory Division. URL: <https://www.fbi.gov/file-repository/laboratory/handbook-of-forensic-services-pdf.pdf/view>.

517. The search and seizure of recordings and the requirement that they be kept under seal in Swiss law DONATSCH ANDREAS¹/NIEDERMANN URSULA². URL: <https://www.ius.uzh.ch/dam/jcr%3A179922a1-59f3-49bc-a30f-01467f329ced/Russisch%20Niedermann.pdf>.

518. Türkmenistanyň Jenaýat Iş Ýörediş Kodeksi. 2009-njy ýylyň 18-nji apreli, № 28-IV (2019-njy ýylyň 1-nji dekabryna çenli girizilen üýtgetmeler we goşmaçalar bilen). Hukuk Maglumatlary Merkezi. URL: <http://minjust.gov.tm/mcenter-single/34>.

519. UK-US agreement under the US CLOUD Act. 7.10.2019. URL: https://www.europarl.europa.eu/doceo/document/E-9-2019-003136_EN.html.

520. UNE EN ISO/IEC 27037:2016. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: <https://www.en-standard.eu/une-en-iso-iec-27037-2016-information-technology-security-techniques-guidelines-for-identification-collection-acquisition-and-preservation-of-digital-evidence-iso-iec-27037-2012-endorsed-by-aenor-in-december-of-2016>.

521. United States v. Ganas, No. 12-240 (2d Cir. 2016). URL: <https://law.justia.com/cases/federal/appellate-courts/ca2/12-240/12-240-2016-05-27.html>.

522. United States Department of Justice. Computer Crime and Intellectual Property Section (CCIPS). Criminal Division Strategic Approach to Countering Cybercrime. URL: <https://www.justice.gov/criminal/criminal-ccips/criminal-division-strategic-approach-countering-cybercrime>.

523. Unodc Cybercrime Module 6 Key Issues: Digital Evidence Admissibility. URL: <https://www.unodc.org/cld/en/education/tertiary/cybercrime/module-6/key-issues/digital-evidence-admissibility.html>.

524. Upgraded Schengen Information System Went Live. URL: <https://eucrim.eu/news/upgraded-schengen-information-system-went-live/>.

525. Using appeal judgement transcripts to assess changes in the presence of digital evidence in police investigations. Published 19 May 2022. URL: <https://www.gov.uk/government/publications/digital-evidence-in-appeal-judgement-transcripts/using-appeal-judgement-transcripts-to-assess-changes-in-the-presence-of-digital-evidence-in-police-investigations>.

526. Veber J. & Smutny Z. Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic. 14th European Conference on Cyber Warfare & Security, Hatfield, UK, 2-3 July 2015. P. 294-299. URL: https://www.researchgate.net/profile/Zdenek-Smutny/publication/283226153_Standard_ISO_270372012_and_Collection_of_Digital_Evidence_Experience_in_the_Czech_Republic/links/569a87dd08ae6169e55b844f/Standard-ISO-270372012-and-Collection-of-Digital-Evidence-Experience-in-the-Czech-Republic.pdf.

527. Virtuelle Kriminalität steigt weiter an: IT-Spezialisten der Polizei gehen erfolgreich gegen Cybercrime vor. URL: <https://www.mi.niedersachsen.de/startseite/aktuelles/presseinformationen/virtuelle-kriminalitaet-steigt-weiter-an-it-spezialisten-der-polizei-gehen-erfolgreich-gegen-cybercrime-vor-243893.html>.

528. Vorschriften im Verfassungsschutzgesetz NRW zur Online-Durchsuchung und zur Aufklärung des Internet nichtig. Urteil vom 27. Februar 2008 – 1 BvR 370/07. URL:

<https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2008/bvg08-022.html>.

529. Wahl T. E-evidence Regulation and Directive Published. URL: <https://eucrim.eu/news/e-evidence-regulation-and-directive-published/>.

530. Watney M. Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position. *J. Inf. Law Technol.*, 2009. URL: <https://www.semanticscholar.org/paper/Admissibility-of-Electronic-Evidence-in-Criminal-An-Watney/ee1ec3411002904e965306f97fb098c4eb2b8e26?utm>.

531. Wetboek van Strafvordering. Geldend van 01-07-2025 t/m heden. Nederland. URL: <https://wetten.overheid.nl/BWBR0001903>.

532. Wilkinson S. Good Practice Guide for Computer-Based Electronic Evidence :Official release version 4.0. 2006. 66 p.

533. Yang F., Feng J., Rules of electronic data in criminal cases in China, *International Journal of Law, Crime and Justice*, Volume 64, 2021. URL: <https://www.sciencedirect.com/science/article/abs/pii/S1756061620304882?utm>.

534. Yankson B., Davis A. Analysis of the Current State of Cloud Forensics: The Evolving Nature of Digital Forensics. In *IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*. 2019. Pp. 1–8. URL: <https://doi.org/10.1109/AICCSA47632.2019.9035336>.

535. Youth Justice and Criminal Evidence Act 1999. URL: <https://www.legislation.gov.uk/ukpga/1999/23/contents>.

536. Yu R. Electronic evidence and electronic discovery in the Hong Kong Special Administrative Region, People's Republic of China. *Digital Evidence and Electronic Signature Law Review*. 13 (2016). p.p. 26-43 URL: <https://journals.sas.ac.uk/deeslr/article/download/2294/2247/0?utm>.

537. Zawoad S., Hasan R. I have the proof: Providing proofs of past data possession in cloud forensics. In 2012 *International Conference on Cyber Security, (SocialInformatics)*. 2012. P. 75–82. URL: <https://doi.org/10.48550/arXiv.1211.4328>.

538. Հայաստանի Հանրապետության քրեական դատավարության օրենսգիրք, Ընդունվել է ՀՀ Ազգային ժողովի կողմից 1 հուլիսի 1998 թ. (համապատասխան ինկորպորացիան՝ ԱԺ,01.07.1998,ՀՕ-248, մայր փաստաթղթին փոփոխող փաստաթղթերը՝ ԱԺ,14.11.2019,ՀՕ-217-Ն). Հայաստանի իրավական տեղեկատվական համակարգ. Armenian legal informational system. URL: <https://www.arlis.am/DocumentView.aspx?docid=136684>.

539. المعلومات تقنية جرائم مكافحة شأن في 2015 لسنة 63 رقم قانون . URL: <https://www.moi.gov.kw/main/content/docs/cybercrime/ar/law-establishing-cyber-crime-dept.pdf>.

540. 김민규·김기범 박혜림·허황 형사전자소송의 성공적 안착을 위한 연구 . Minkyu Kim, Gibum Kim, Herim Park, Hwang Heo. Successful Transition to Electronic Criminal Litigation in Korea. December 31, 2023. URL: https://www.kicj.re.kr/board.es?act=view&bid=0029&list_no=14170&mid=a20201000000.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

Монографія

1. Каланча І. Г. Докази, що мають електронну форму, в кримінальному процесі України: концептуальний аспект : монографія. Київ : Вид-во «SBA Print», 2025. 528 с.

Рецензія: Цимбал Г. П. Рецензія на монографію Каланчі Інги Георгіївни «Докази, що мають електронну форму, в кримінальному процесі України: концептуальний аспект». *Європейський правничий часопис*. №10. С. 11–13.

Публікації у виданнях, які включено до наукометричних баз Scopus і Web of Science:

1. Patreliuk D., Svoboda I., Kalancha I., Filashkin V., Kachmar B. Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations. *Pakistan Journal of Life and Social Sciences*. 22(2). 2024. pp. 4811–4820. URL: <https://www.scopus.com/pages/publications/85204286465>.

2. Kozii V.; Kalancha I.; Vlasova H.; Orlean A. Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies. *IDP. Internet, Law an Politics Journal*. no. 42. 2025. pp. 1–13. URL: <https://www.scopus.com/pages/publications/85217974797>.

3. Kalancha I., Bozhyk V., Muzychenko O., Vatsiyk V. Digital evidence in comparative criminal procedure: international experience and the practice of judicial review. *TPM – Testing, Psychometrics, Methodology in Applied Psychology*. Vol. 32, No. S2. 2025. pp. 34–46. URL: <https://www.scopus.com/pages/publications/105013864919>.

Публікації у фахових періодичних виданнях України (категорія «Б»):

1. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Азербайджану. *Науковий вісник Ужгородського національного університету. Серія «Право»*. № 59. 2019. С. 117–121. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2020/12/No.59-2.pdf>.

2. Каланча І. Г. Електронний сегмент кримінального процесу Естонії. *Порівняльно-аналітичне право*. № 3. 2019. С. 212–216. URL: https://pap-journal.in.ua/wp-content/uploads/2021/07/3_2019.pdf.

3. Столітній А. В., Каланча І. Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. Вип. 146. 2019. С. 179–191. URL: <https://doi.org/10.21564/2414-990x.146.171218>.

4. Каланча І. Г. Електронний сегмент в кримінальному процесі Грузії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. № 4. 2019. С. 161–166. URL: <https://doi.org/10.31733/2078->

[3566-2019-4-161-166.](#)

5. Каланча І. Г. Роль правових актів Європейського суду з прав людини в кримінальному процесі України. *Проблеми законності*. Вип. 150. 2020. С. 233–243. URL: <https://doi.org/10.21564/2414-990x.150.209071>.

6. Каланча І. Г. Тенденції та динаміка застосування практики Європейського суду з прав людини під час кримінального провадження: статистичне та соціологічне дослідження. *Теорія і практика правознавства*. Вип. 2(18). 2020. С. 1–17. URL: <https://doi.org/10.21564/2225-6555.2020.18.213676>.

7. Каланча І. Г. Поняття практики Європейського суду з прав людини як джерела кримінального процесуального права України. *Вісник кримінального судочинства*. № 2. 2020. С. 8–21. URL: <https://doi.org/10.17721/2413-5372.2020.3-4/8-21>.

8. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Туркменістану. *Актуальні проблеми вітчизняної юриспруденції*. № 1. 2020. С. 91–95. URL: http://apnl.dnu.in.ua/1_2020/23.pdf.

9. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Вірменії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. № 1. 2020. С. 205–210. URL: <https://visnik.dduvs.edu.ua/index.php/visnyk/issue/view/48/19>.

10. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законі Латвії. *Криміналістика і судова експертиза : міжвідомчий науково-методичний збірник*. Вип. 65. 2020. С. 90–100. URL: https://digest.kndise.gov.ua/wp-content/uploads/2025/07/2020_65.pdf.

11. Каланча І. Г., Гаркуша А. М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*. № 8. 2021. С. 336–339. URL: <https://doi.org/10.32782/2524-0374/2021-8/77>.

12. Каланча І. Г., Орлеан А. М. Адаптація системи кримінальної юстиції до цифровізації світу: роль навчального компоненту. *Наукові перспективи*. № 11(53). 2024. С. 937–944. URL: [https://doi.org/10.52058/2708-7530-2024-11\(53\)-937-944](https://doi.org/10.52058/2708-7530-2024-11(53)-937-944).

13. Каланча І. Г., Юрчишин Ю. В. Забезпечення безпеки прокурора під час роботи з електронним сегментом кримінального провадження в Україні. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки*. Том 35 (74) № 6. 2024. С. 108–115. URL: <https://doi.org/10.32782/TNU-2707-0581/2024.6/19>.

14. Каланча І. Г. Алгоритм електронного кримінального провадження. *Law. State. Technology*. Вип. 4. 2024. С. 69–74. URL: <https://doi.org/10.32782/LST/2024-4-13>.

15. Каланча І. Г. Практика роботи з доказами, що мають електронну форму в кримінальному процесі України: соціологічне дослідження. *Успіхи і досягнення у науці*. № 1 (11). 2025. С. 76–93. URL: [https://doi.org/10.52058/3041-1254-2025-1\(11\)-76-93](https://doi.org/10.52058/3041-1254-2025-1(11)-76-93).

16. Каланча І. Г., Стемковський Д. Б. Використання доказів, що мають

електронну форму в кримінальному процесі України: судова практика. *Аналітично-порівняльне правознавство*. № 2. 2025. С. 1001–1008. URL: <https://doi.org/10.24144/2788-6018.2025.02.148>.

17. Каланча І. Г. Електронний висновок експерта як доказ у кримінальному процесі України: практика, перспективи та ризики. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. № 2. 2025. С. 84–92. URL: <https://doi.org/10.32782/2311-8040/2025-2-12>.

18. Каланча І. Г. Процесуальна природа доказів, що мають електронну форму в кримінальному процесі України: документ та речовий доказ. *Міжнародний науковий журнал "Інтернаука". Серія: "Юридичні науки"*. № 7. 2025. С. 85–92. URL: <https://doi.org/10.25313/2520-2308-2025-7-11208>.

19. Каланча І. Г. Організаційні аспекти роботи з доказами, що мають електронну форму в кримінальному процесі України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. Вип. 90. Ч. 4. 2025. С. 258–266. URL: <https://doi.org/10.24144/2307-3322.2025.90.4.36>.

Публікації у періодичних виданнях іноземних держав:

1. Каланча І. Г. Електронний сегмент в кримінальному процесуальному законодавстві Молдови. *Jurnalul Juridic National: teorie si practica*. № 1 (41). 2020. С. 132–137. URL: <http://www.jurnaluljuridic.in.ua/archive/2020/1/30.pdf>.

2. Каланча І. Г. Інтегровуваність як обов'язкова властивість електронних інформаційних систем органів кримінальної юстиції. *Ročenka Ukrajinsko-Slovenská. Zborník vedeckých prác*. (Рочник Українсько-Словацький. Збірник наукових праць) 2020. С. 64–70. URL: <https://www.eeda.sk/dok/publikacie/ostatne/2020-rocenka-ukrajinsko-slovenska.pdf>.

3. Каланча І. Г. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світлі концепції chain of custody. *Věda a perspektivy*. № 8 (51). 2025. С. 206–230. URL: [https://doi.org/10.52058/2695-1592-2025-8\(51\)-206-230](https://doi.org/10.52058/2695-1592-2025-8(51)-206-230).

Тези виступів на науково-практичних конференціях:

1. Каланча І. Г. Єдине електронне інформаційне поле органів кримінальної юстиції. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : матер. міжн. наук.-практ. конф. (м. Київ, 05.11.2019 р.). Київ, 2019. С. 209–213. URL: https://www.researchgate.net/publication/393743748_Kalanca_IG_Edine_elektronne_informacijne_pole_organiv_kriminalnoi_usticii_Aktualni_pitanna_sudovoi_ekspertologii_kriminalistiki_ta_kriminalnogo_procesu_mat_mizn_nauk-prakt_konf_m_Kiiv_5112019_r_K_2019.

2. Каланча І. Г. Шляхи формування сучасних практичних

компетентностей у випускників правничих шкіл України. *Інноваційні рішення в сучасній науці, освіті та практиці*: матеріали I Міжнародної науково-практичної інтернет-конференції (наукове видання), 17–18 листопада 2020 р.: у 2 ч. Київ: НТУ, 2020. Ч. 2. С. 209–212. URL: <http://vstup.ntu.edu.ua/conf-innov-part-2.pdf>.

3. Гаркуша А. М., Каланча І. Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи*: матеріали круглого столу (м. Львів, 11 червня 2021 р.). Львів: Львівський державний університет внутрішніх справ., 2021. С. 159–165. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/11_06_2021.pdf.

4. Каланча І. Г. Підходи до класифікації електронних носіїв інформації та інформаційних систем для завдань кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: матеріали V Міжнар. наук.-практ. конф. (29 жовтня 2021 р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2021. С. 211–213. URL: <https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk-29.10.21.pdf>.

5. Гаркуша А. М., Каланча І. Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. *Наукові читання пам'яті Ганса Гросса*: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 9 грудня 2021 р.). Чернівці : Технодрук, 2021. С. 72–75. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/11383/Forensic_Epi_stemology_Czernowitz_2021_.pdf?sequence=1&isAllowed=y.

6. Каланча І. Г. Окремі аспекти діяльності прокурора щодо гарантування цілісності доказів, що мають електронну форму під час досудового розслідування кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: матеріали VI Міжнар. наук.-практ. конф. (21 жовтня 2022р., Чернівці)/ редкол.: О. В. Щербанюк та ін. Чернівці, 2022. С. 327–332. URL: https://ccu.gov.ua/sites/default/files/suchasni_vyklyky_ta_aktualni_problemy_sudo_voyi_reformy_v_ukrayini_2022.pdf.

7. Каланча І. Г. Способи ідентифікації комп'ютерних даних як доказу в кримінальному провадженні. *III Наукові читання пам'яті Ганса Гросса* : збірник тез міжнар. науково-практичної конференції (м. Чернівці, 8 грудня 2023 р.). Чернівці: Чернівець. нац. у-нт ім. Ю.Федьковича, 2023. С. 71–75. URL: <https://www.ndekc.cv.ua/wp-content/uploads/2024/03/III-Naukovi-chytannya-pam-yati-Gansa-Grossa.pdf>.

8. Каланча І. Г. Стратегії фіксації доказів, що мають електронну форму для застосування в кримінальному провадженні. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VII Міжнар. наук.-практ. конф. (27 жовтня 2023 р., Чернівці)/ редкол.: О. В. Щербанюк та ін. Чернівці: 2023. С. 253–258. URL: https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk_conf_27..pdf.

9. Каланча І. Г. Кіберпростір як територія проведення досудового

розслідування. *Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини*: зб. наук. праць за матер. Круглого столу, Київ, 7 грудня 2023 р. / редкол.: А. Ю. Нашинець-Наумова, Г. П. Власова, С. В. Бобровник, Т. О. Дідич, Н. А. Сергієнко, А. П. Чернега. Київ : Київ. стол. ун-т ім. Б. Грінченка, 2024. С. 115–119. URL: <https://kubg.edu.ua/struktura/pidroz dili/yurydychna-klinika-astreya/zakhody/8438-ikh-kruhlyi-stil-prava-liudyny-v-umovakh-voiennoho-stanu-v-ukraini.html>.

10. Каланча І. Г. Цифрова складова кримінального процесу України в науці та практиці: структурно-функціональний аналіз. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VIII Міжнар. наук.-практ. конф. (31 жовтня 2024р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2024. С. 229–233. URL: https://www.researchgate.net/publication/390005117_Kalanca_IG_Cifrova_sklado_va_kriminalnogo_procesu_Ukraini_v_nauci_ta_praktici_strukturno-funkcionalnij_analiz_Sucasni_vikliki_ta_aktualni_problemi_sudovoi_reformi_v_Ukraini_Materiali_VIII_Miznar_nauk-p.

11. Каланча І. Г. Матеріальна форма існування як властивість доказу в кримінальному процесі України: практика правозастосування. *Права людини в умовах воєнного стану в Україні: Х круглий стіл до Всеукраїнського тижня права (10 грудня 2024 року). Права людини в умовах воєнного стану в Україні: до тижня права і Загальної декларації прав людини* : зб. наук. праць за матер. круглого столу, Київ, 10 грудня 2024 р. / редкол.: А.Ю. Нашинець-Наумова, Г.П. Цимбал, С.В. Бобровник, Т.О. Дідич, О.І. Чаплук, А.П. Чернега. Київ : Київ. столич. ун-т ім. Б. Грінченка, 2025. С. 63–67. URL: https://www.researchgate.net/publication/396154856_Kalanca_IG_Materialna_forma_isnuvanna_ak_vlastivist_dokazu_v_kriminalnomu_procesi_Ukraini_praktika_pravozastosuvanna_Prava_ludini_v_umovah_voennogo_stanu_v_Ukraini_X_kruglij_stil_do_Vseukrainskogo_tiz.

12. Каланча І. Г. Результати OSINT як джерело доказів у кримінальному процесі України. *Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій*: матеріали Всеукр. наук.-практ. конф. (м. Чернівці, 20 грудня 2024 р.) / відп. ред. К.А. Возняковська. ТОМ 1, Чернівці, 2024. С. 43–49. URL: https://www.researchgate.net/publication/389647938_Kalanca_IG_Rezultati_OSINT_ak_dzerelo_dokaziv_u_kriminalnomu_procesi_Ukraini_Innovacii_vikliki_ta_novi_gorizonti_pravovogo_reguluvanna_u_svitli_sucasnih_socialno-ekonomichnih_ta_politichnih_transformaci.

13. Каланча І. Г. Використання висновку експерта, що має електронну форму як доказу в кримінальному процесі України. *Актуальні проблеми національного законодавства*: збірник матеріалів Міжнародної науково-практичної конференції, м. Кропивницький, 17 квітня 2025 року. Частина 1. Кропивницький, 2025. С. 154–156. URL: https://www.researchgate.net/publication/392901845_Kalanca_IG_Vikoristanna_v_isnovku_eksperta_so_mae_elektronnu_formu_ak_dokazu_v_kriminalnomu_proces

i Ukraini Aktualni problemi nacionalnogo zakonodavstva zbirnik materialiv Miznarodnoi naukovo-prakticno.

14. Каланча І. Термінологічне розмежування понять «електронний доказ», «цифровий доказ» і «доказ, що має електронну форму» в кримінальному процесі України. *Пріоритетні шляхи розвитку науки і освіти: матеріали XV Міжнародної науково-практичної конференції* (м. Львів, 9–10 травня 2025 року). Львів : Львівський науковий форум, 2025. С. 195-197. URL: <http://www.lviv-forum.inf.ua/save/2025/9-10.05/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA.pdf>.

15. Власова Г. П., Каланча І. Г. Захисник як суб'єкт роботи з електронними доказами в кримінальному провадженні. *Актуальні питання реформування правової системи* : зб. матеріалів XXII Міжнар. наук.-практ. конф., Луцьк, 13-15 червня 2025 р. / Уклад. Джурак Л. М. Луцьк : Вежа-Друк, 2025. С. 113–115. URL: https://www.law.vnu.edu.ua/files/ugd/65dd18_5ab2de833d004115b0483aa2420d7cc0.pdf.

Праці, які додатково відображають результати дослідження:

1. Каланча І. Г. Організація навчання представників органів кримінальної юстиції сучасним процесуально-цифровим компетентностям. *Training legal professionals following European standards: scientific and pedagogical internship*, November 4 – December 15, 2024. Riga, the Republic of Latvia. p.p. 45-50.

2. Каланча І. Г., Щербанюк О. В. Досудовий процес. Навчально-методичний посібник. Чернівці: Рута. Чернівецький національний університет імені Юрія Федьковича, 2020. 200 с.

3. Шевчук П. В., Каланча І. Г. Кримінальний процес : навчально-методичний посібник для здобувачів вищої освіти першого (бакалаврського) рівня; галузь знань – 08 «Право»; спеціальність – 081 «Право». Чернівці, 2024. 184 с.

Опитування щодо практики роботи з доказами, що мають електронну форму в кримінальному провадженні

Це опитування розроблено та проводиться к.ю.н. Каланчею І.Г. в рамках наукового дослідження практики роботи з доказами, що мають електронну форму в кримінальному провадженні.

Опитування є анонімним, будь-які персональні дані (електронні адреси, персоналізовані відповіді тощо) скремо не публікуватимуться та не передаватимуться.

Узагальнені результати опитування буде опубліковано з дотриманням вимог академічної доброчесності.

Дякую Вам за участь!

Зірочка () указує, що запитання обов'язкове*

1. Оберіть Вашу професію *

Виберіть рос, що підходить.

- ☐ Суддя
- ☐ Прокурор
- ☐ Адвокат
- ☐ Слідчий / Детектив
- ☐ Експерт / Спеціаліст
- ☐ Науковець
- ☐ Інше: _____

2. Вкажіть місце Вашої роботи (за бажанням)

3. Який у Вас досвід роботи в галузі права? *

Виберіть лише один варіант.

- ☐ до 3 років
- ☐ до 5 років
- ☐ понад 5 років
- ☐ понад 10 років
- ☐ понад 15 років
- ☐ понад 20 років
- ☐ понад 25 років
- ☐ понад 30 років
- ☐ Інше: _____

4. Як часто Ваша робота пов'язана з доказами, що мають електронну форму? *

Виберіть лише один варіант.

- ☐ дуже часто (понад 90%)
- ☐ часто (близько 70%)
- ☐ час від часу (близько 50%)
- ☐ рідко (близько 30 %)
- ☐ дуже рідко (менше 10%)
- ☐ не пов'язана
- ☐ інше: _____

5. З якою сферою права пов'язана Ваша робота з доказами, що мають електронну форму? *

Виберіть лише один варіант.

- ☐ кримінальна
- ☐ цивільна
- ☐ адміністративна
- ☐ господарське
- ☐ кілька одночасно
- ☐ інше: _____

6. Які типи електронних доказів у Вашій практиці збираються (отримуються) в кримінальних провадженнях? *

Виберіть усі, що підходять.

- ☐ Електронні документи (юридичні документи з використанням електронних підписів, електронних сертифікатів походження або внутрішніх міток організації/сервісів)
- ☐ Програмні коди, програмні логи (запис діяльності, порушень програмного продукту), результати програмного продукту (результати обробки інформації, запитів до сервісів тощо)
- ☐ Результати фіксування: відеозаписи, фотознімки, аудіозаписи, відскановані документи тощо
- ☐ Електронне листування: листування через месенджери, електронну пошту, внутрішні сервіси сервера (внутрішні месенджери продукту для комунікації з операторами, іншими клієнтами тощо)
- ☐ інше: _____

7. Чи використовується у Вашій роботі певна стандартизована інструкція/процедура для фіксації джерела надходження електронного доказу (протоколювання та долучення до матеріалів кримінального провадження)? *

Виберіть лише один варіант.

☐ Так

☐ Ні

☐ Інше: _____

8. Яку процедуру фіксації джерела надходження електронного доказу Ви застосовуєте у своїй роботі? (напишіть коротку відповідь) *

9. Чи використовується у Вашій роботі певна стандартизована інструкція/процедура для перевірки цілісності (достовірності) доказу, що має електронну форму? *

Виберіть лише один варіант.

☐ Так

☐ Ні

☐ Інше: _____

10. Яку процедуру перевірки цілісності (достовірності) доказів, що мають електронну форму Ви застосовуєте у своїй роботі? (напишіть коротку відповідь) *

11. Як у Вашій практиці відбувається зберігання доказів та їх долучення до матеріалів кримінального провадження (можна обрати кілька варіантів відповідей)? *

Виберіть усі, що підходять.

☐ Копіювання або вилучення доказів

☐ Зберігання доказів після долучення (на фізичних носіях (ПК або фізичні носії інформації (флешки, диски, жорсткі диски тощо), на хмарних сервісах)

☐ Систематизація доказів для подальшого використання

☐ Додання доказів до внутрішніх систем відомства

☐ Інше: _____

12. Чи присутня у Вашій роботі практика використання одних і тих же доказів, що мають електронну форму в кількох кримінальних провадженнях? *

Виберіть лише один варіант.

- ☐ Так, дублювання документів
- ☐ Так, повторне допущення як доказу по справі
- ☐ Ні
- ☐ Інше: _____

13. З якими проблемами Ви зіштовхуєтесь у роботі з доказами, що мають електронну форму? (можна обрати декілька варіантів) *

Виберіть усі, що відносяться.

- ☐ Процесуальна некомпетентність колег у питанні доказів, що мають електронну форму
- ☐ Технічна некомпетентність колег у питанні доказів, що мають електронну форму
- ☐ Безпека зберігання цифрових доказів
- ☐ Тегування (виділення важливих рис як дата, час, місце, сервіс отримання тощо для подальшого зручного пошуку) доказів, що мають електронну форму
- ☐ Технічні аспекти зберігання доказів, що мають електронну форму (наявність носіїв інформації, захищених сейфів/кімнат тощо)
- ☐ Передача доказів, що мають електронну форму іншим органам /особам
- ☐ Використання доказів, що мають електронну форму в інших кримінальних провадженнях
- ☐ Використання доказів, що мають електронну форму в суді
- ☐ Інше: _____

14. Чи існує, на Вашу думку, необхідність створення електронної системи для збирання та зберігання цифрових доказів, що міститиме в своєму функціоналі можливості пошуку (наприклад, надсилення електронних запитів) у межах всіх/більшості кримінальних проваджень (для подальшого використання можливих доказів)? *

Виберіть лише один варіант.

- ☐ Так
- ☐ Ні
- ☐ Інше: _____

15. Чи виникає у Вашій роботі необхідність звертатись до колег для пошуку доказів, що мають електронну форму? (напишіть будь ласка розгорнуту відповідь) *

16. Які проблеми найчастіше виникають при збиранні, перевірці та оцінці доказів, що мають електронну форму? (напишіть будь ласка розгорнуту відповідь) *

17. Чи вважаєте Ви достатніми свої знання щодо доказів, що мають електронну форму? *

Виберіть лише один варіант.

☐ Так

☐ Ні

☐ Інше: _____

18. Чи проходили Ви навчання / тренінги / підвищення кваліфікації з питань доказів, що мають електронну форму? *

Виберіть лише один варіант.

☐ Так

☐ Ні

☐ Інше: _____

19. Якщо Ви проходили навчання / тренінги / підвищення кваліфікації з питань доказів, що мають електронну форму - вкажіть де саме та поділіться будь ласка Вашими враженнями, порадами, рекомендаціями, пропозиціями

20. Яка форма отримання знань щодо доказів, що мають електронну форму оптимальна для Вас? *

Виберіть лише один варіант.

- ☐ Лекції та семінари
- ☐ Письмові матеріали (методичні рекомендації, статті тощо)
- ☐ Очні тренінги
- ☐ Он-лайн тренінги
- ☐ Короткі відео-лекції
- ☐ Інше: _____

21. Ви також можете вказати Ваші зауваження, рекомендації або пропозиції за темою опитування, електронну адресу для зворотного зв'язку (за бажанням)

Компанія Google не створювала цей вміст і не підтримує його.

Google Форми

Додаток В

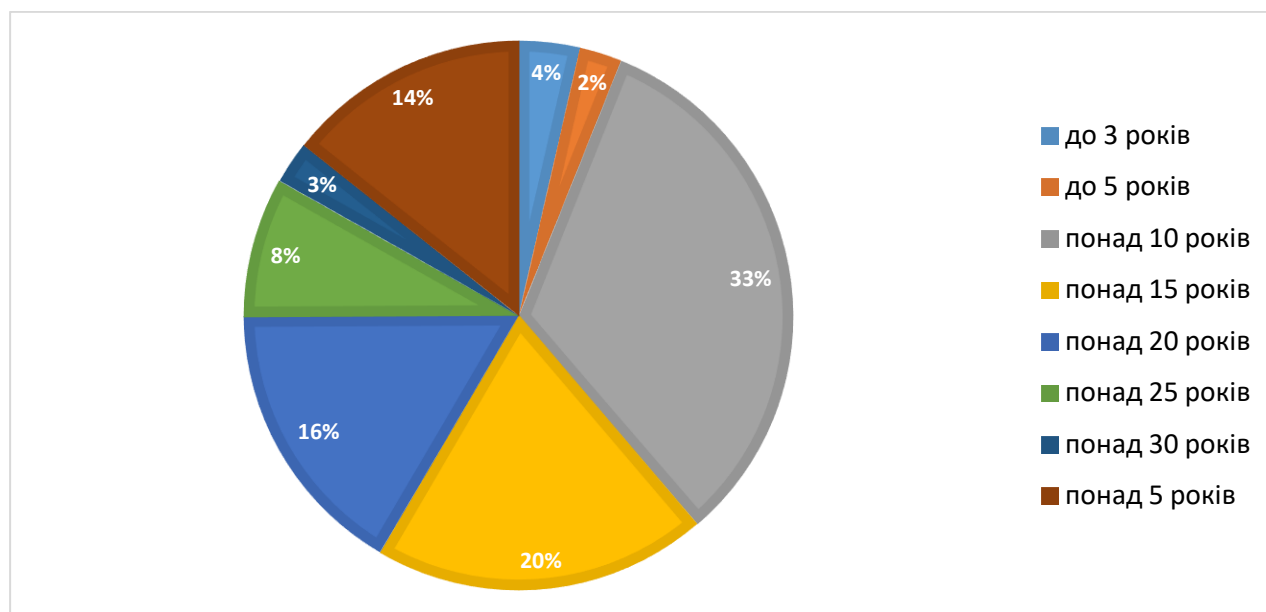


Рис. 1. Досвід респондентів щодо роботи в галузі права

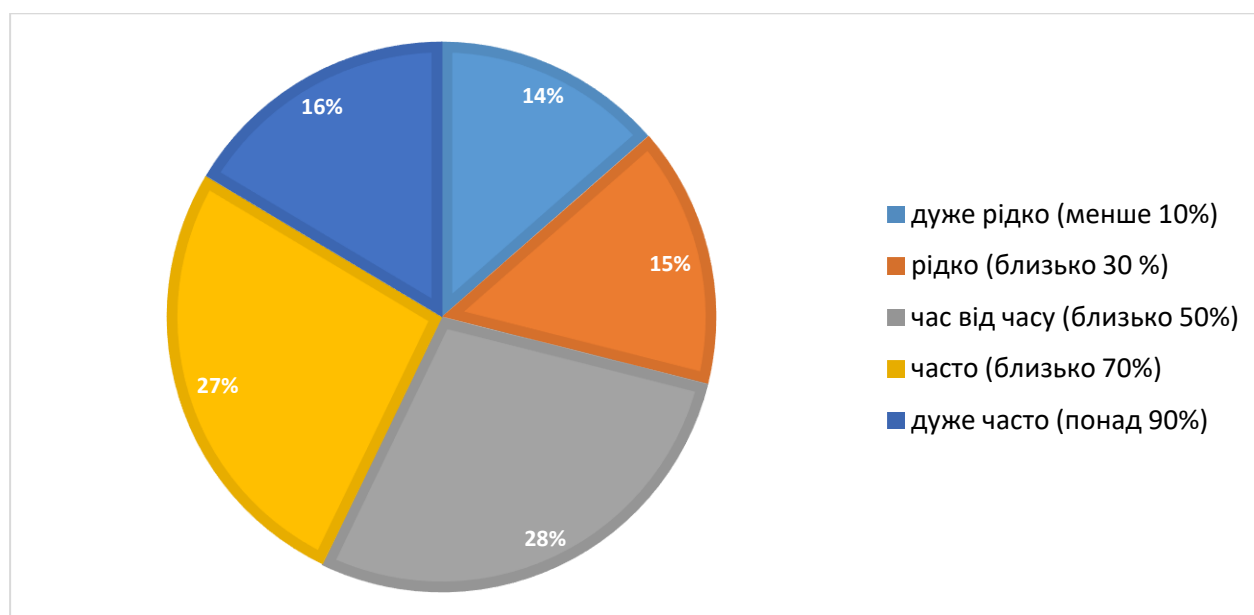


Рис. 2. Ступінь залученості респондентів до роботи з доказами, що мають електронну форму



Рис. 3. Типи доказів, що мають електронну форму в практиці правозастосування

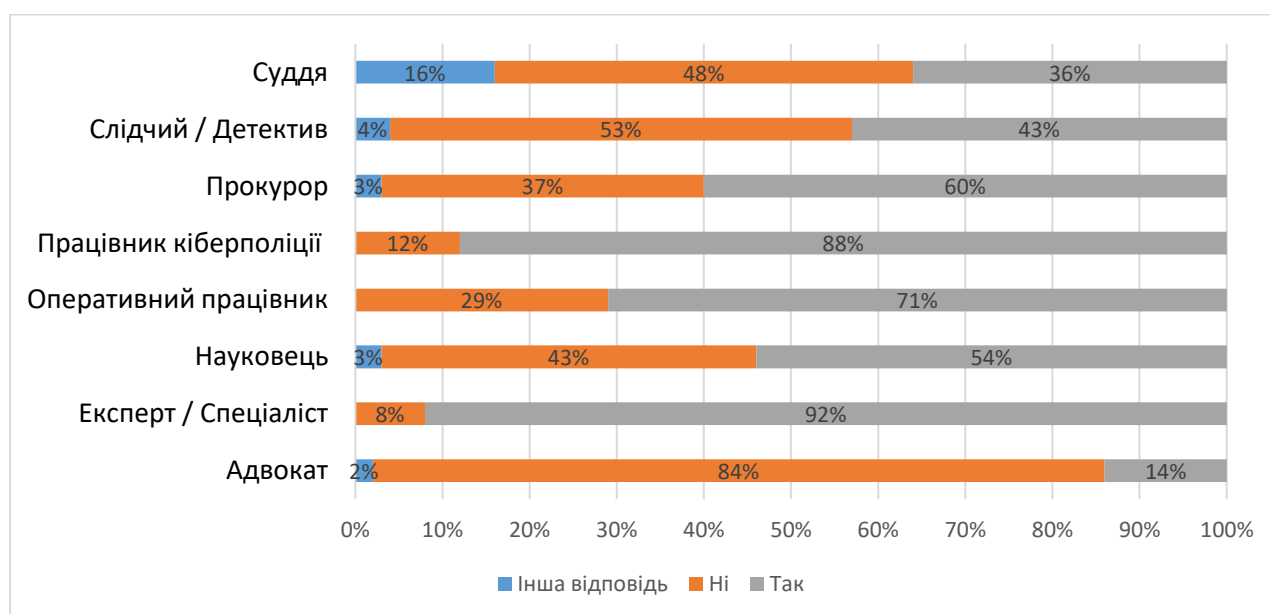


Рис. 4. Стан використання стандартизованих інструкцій/процедур для фіксації джерела надходження електронного доказу



Рис. 5. Різновиди процедур фіксації джерела надходження електронного доказу, що застосовуються під час кримінального провадження

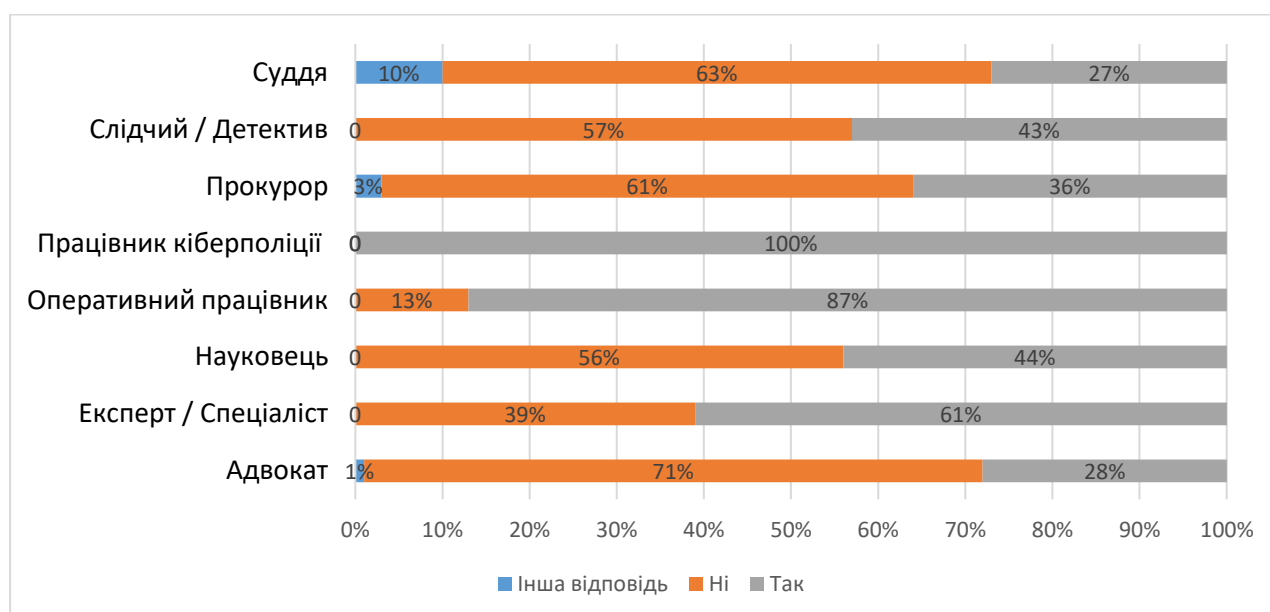


Рис. 6. Стан використання стандартизованих інструкцій/процедур для перевірки цілісності (достовірності) доказу



Рис. 7. Різновиди процедур перевірки цілісності (достовірності) доказів, що мають електронну форму, що застосовуються під час кримінального провадження

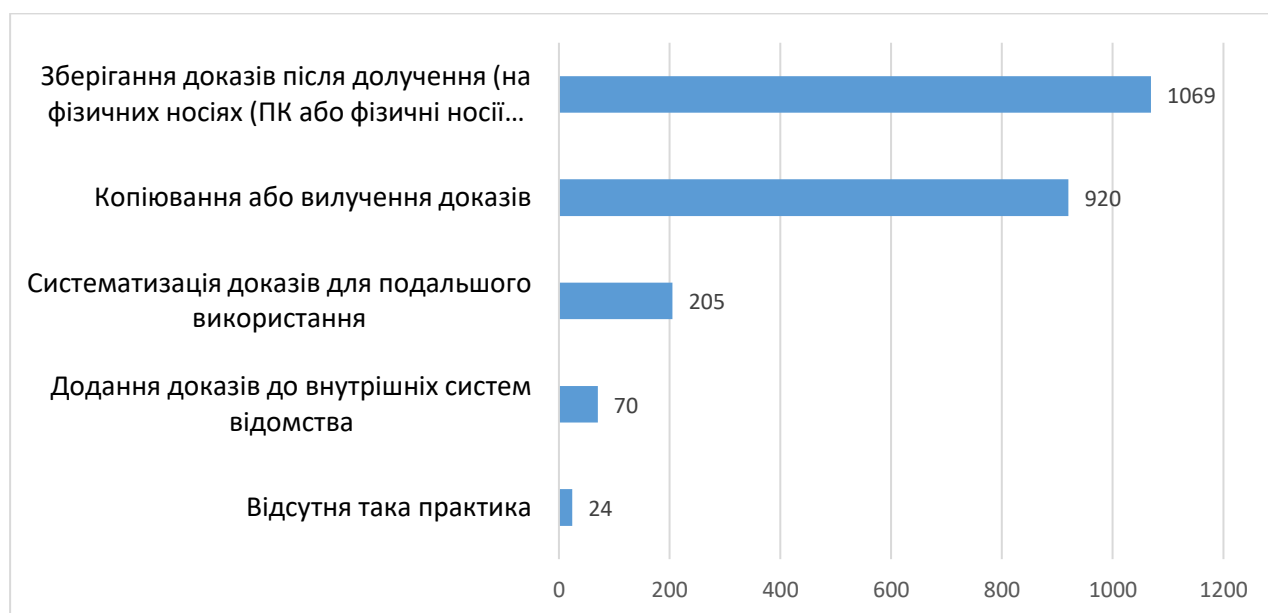


Рис. 8. Різновиди практики зберігання доказів та їх долучення до матеріалів кримінального провадження



Рис. 9. Практика використання одних і тих же доказів, що мають електронну форму в кількох кримінальних провадженнях



Рис. 10. Проблемні питання під час роботи з доказами, що мають електронну форму

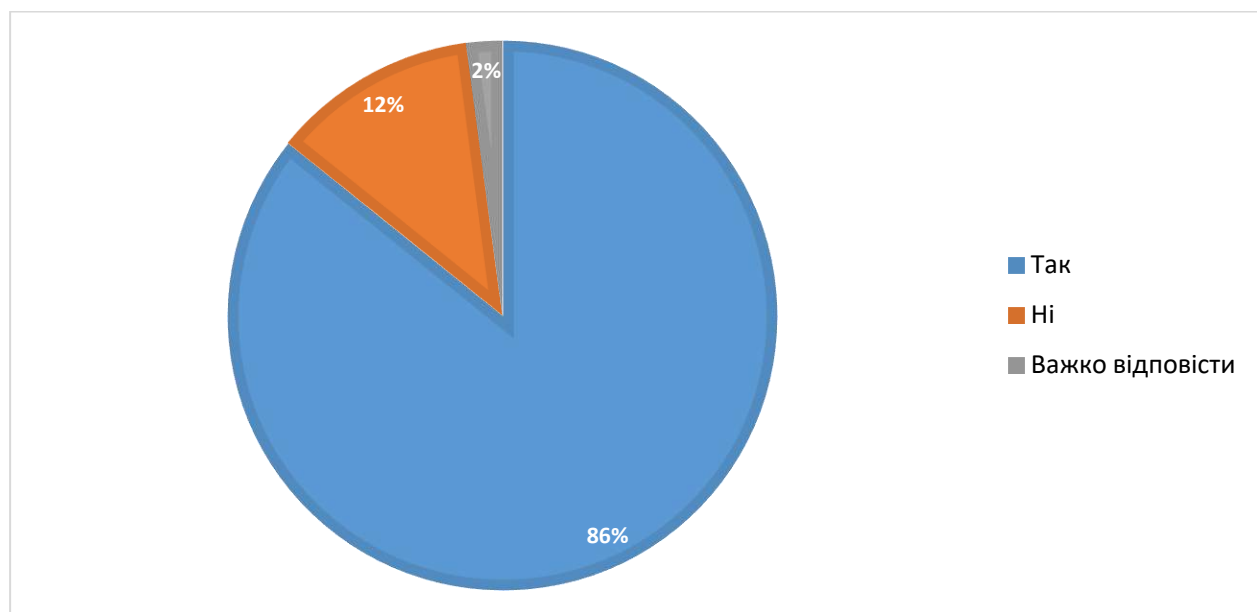


Рис. 11. Оцінка необхідності створення електронної системи для збирання та зберігання цифрових доказів, що міститиме в своєму функціоналі можливості пошуку у межах всіх/більшості кримінальних проваджень

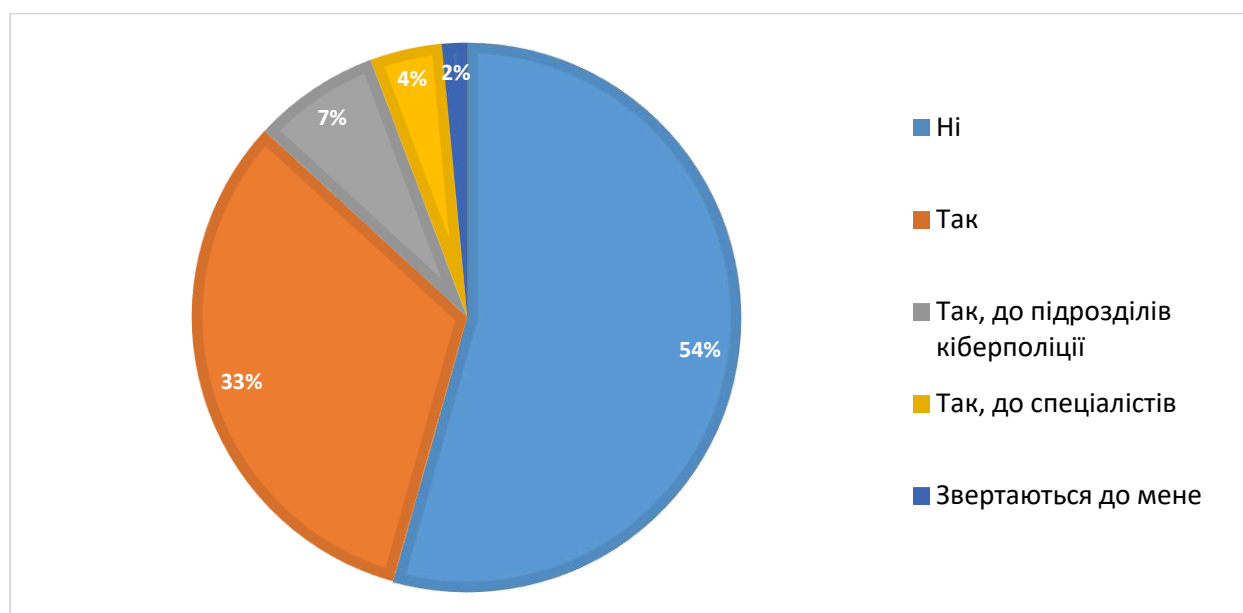


Рис. 12. Оцінка необхідності звертатись до колег для пошуку доказів, що мають електронну форму



Рис. 13. Проблемні питання, що виникають при збиранні, перевірці та оцінці доказів, що мають електронну форму

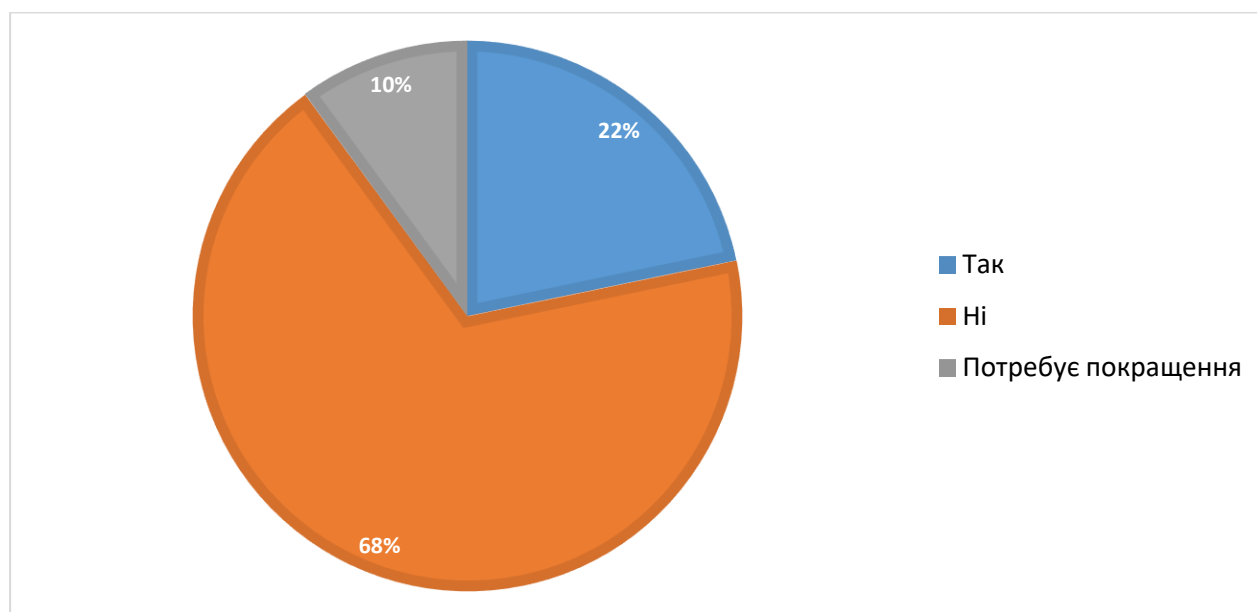


Рис. 14. Оцінка достатності рівня знань щодо доказів, що мають електронну форму

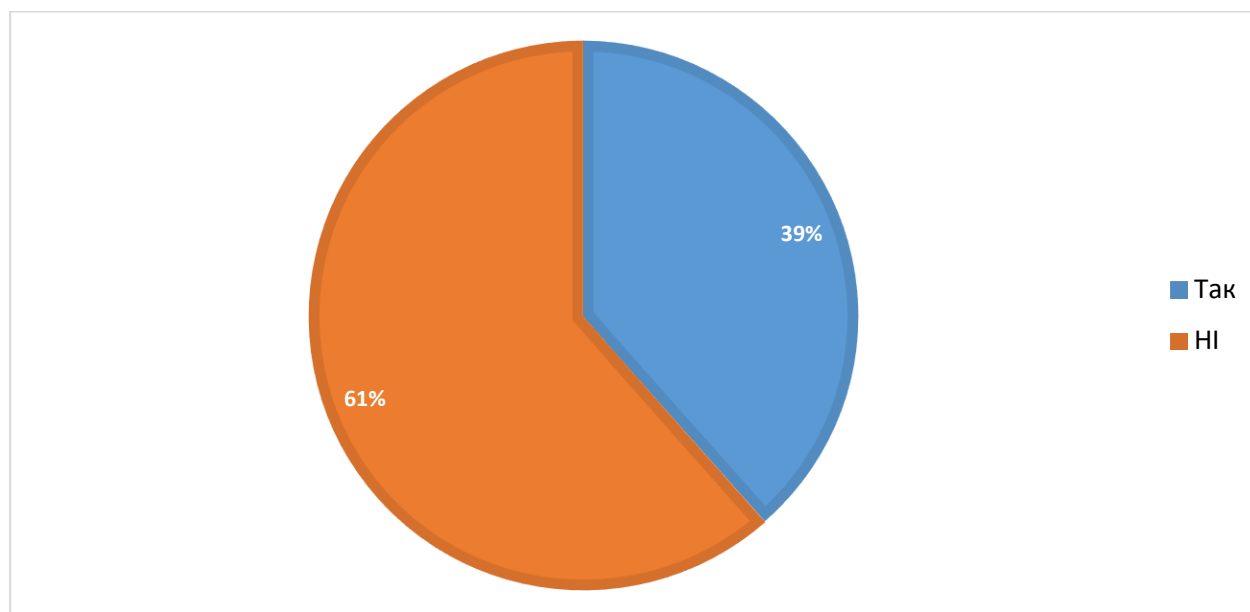


Рис. 15. Проходження респондентами навчання / тренінгів / підвищення кваліфікації з питань доказів, що мають електронну форму

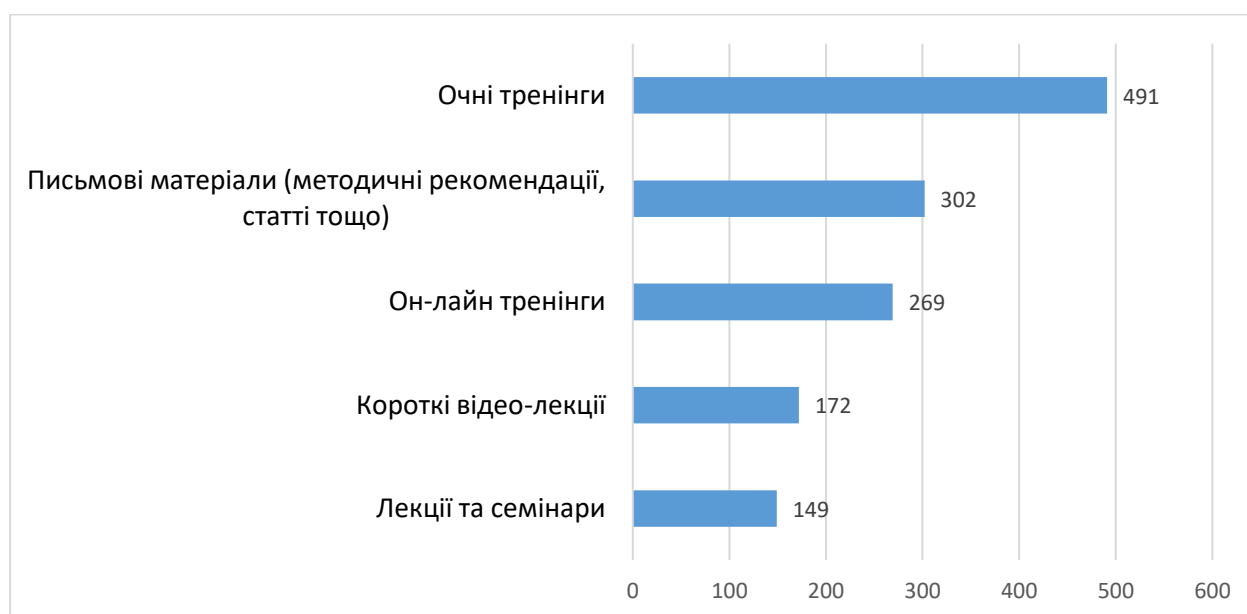
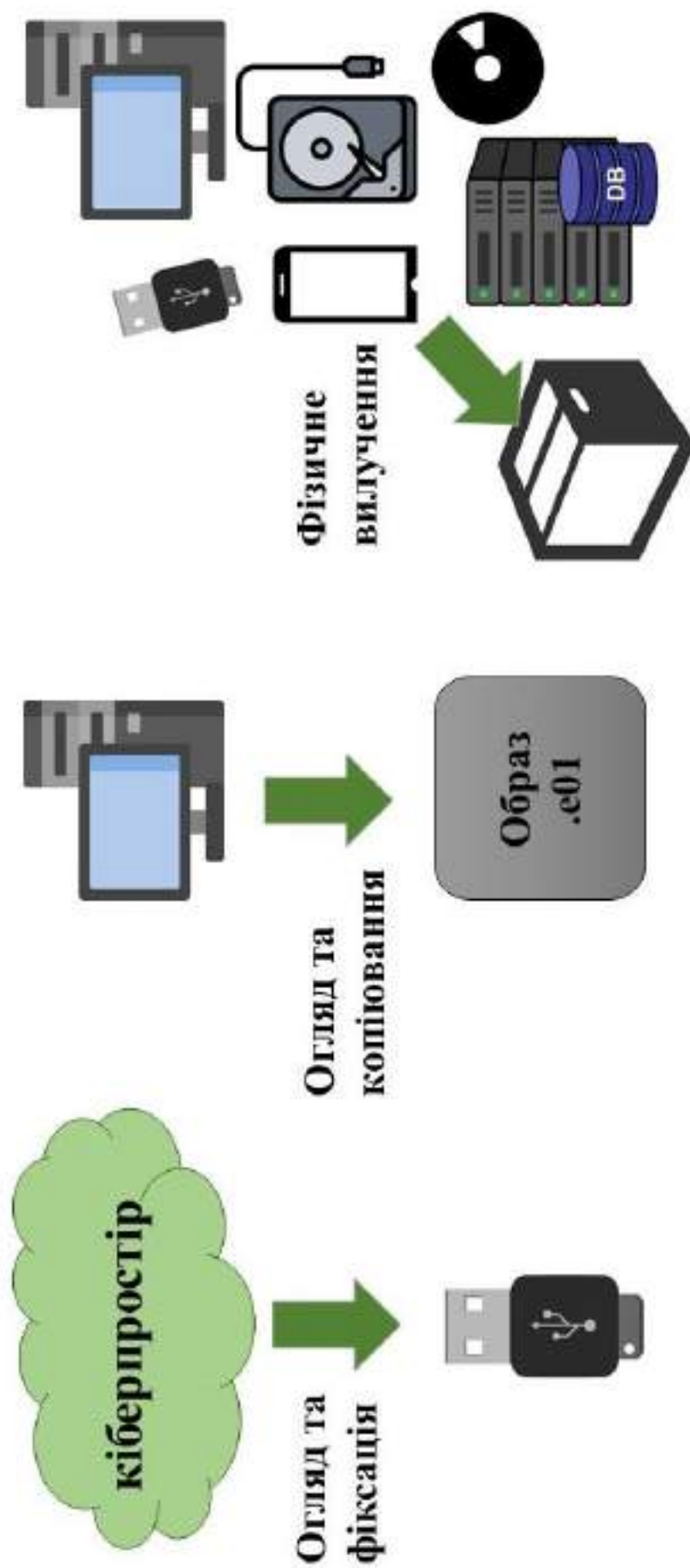
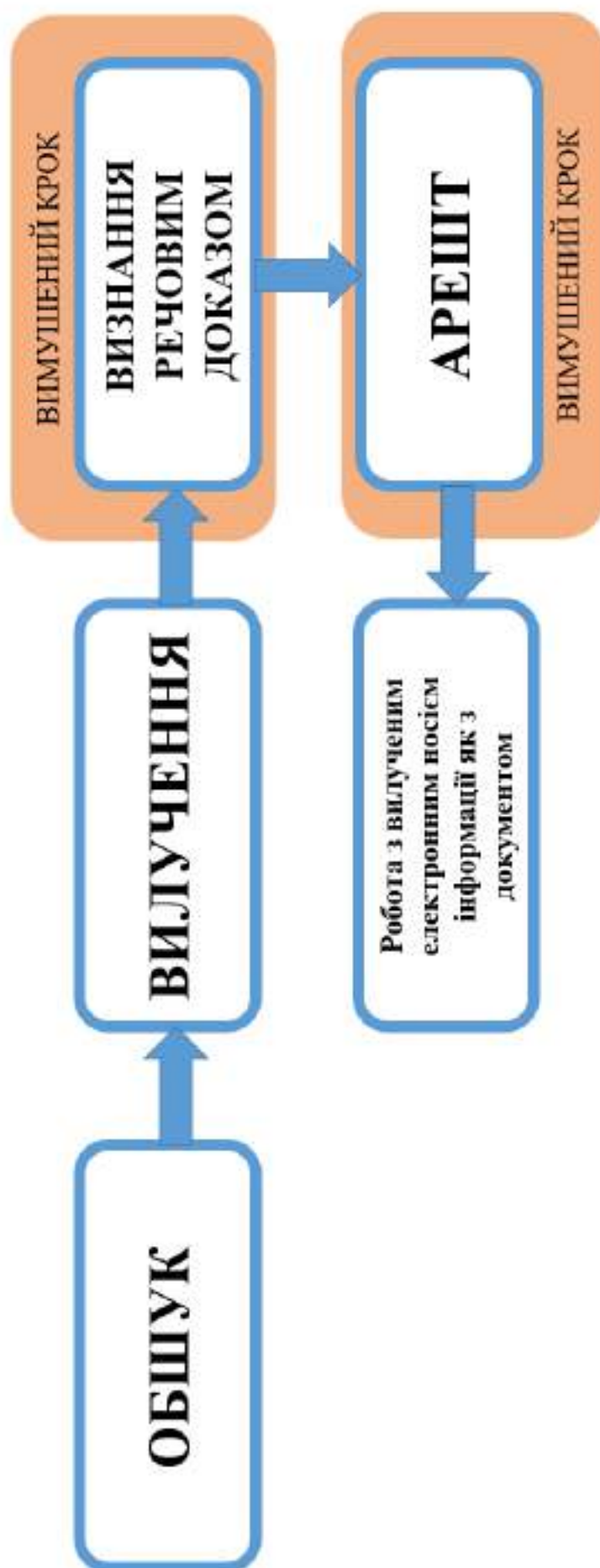
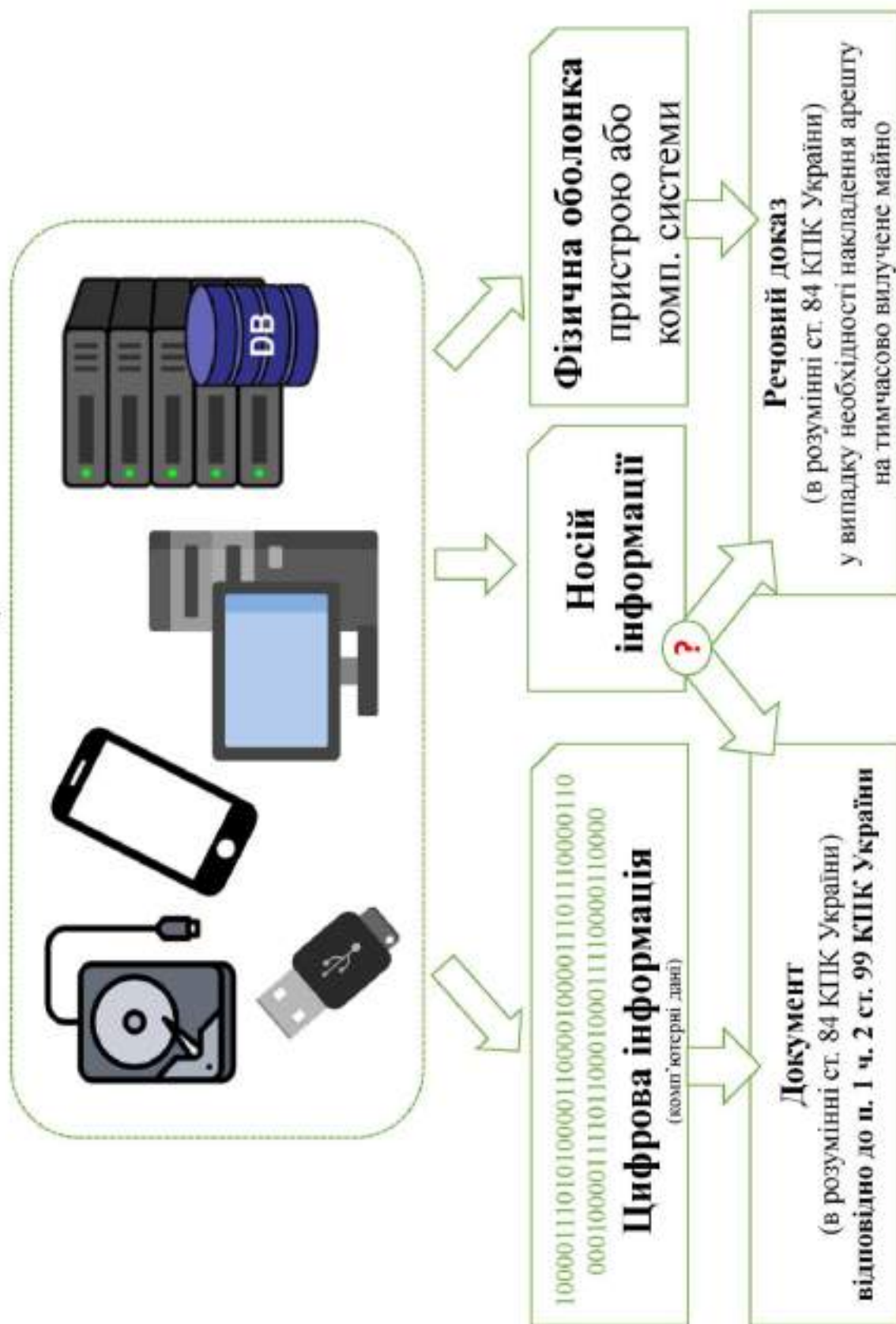


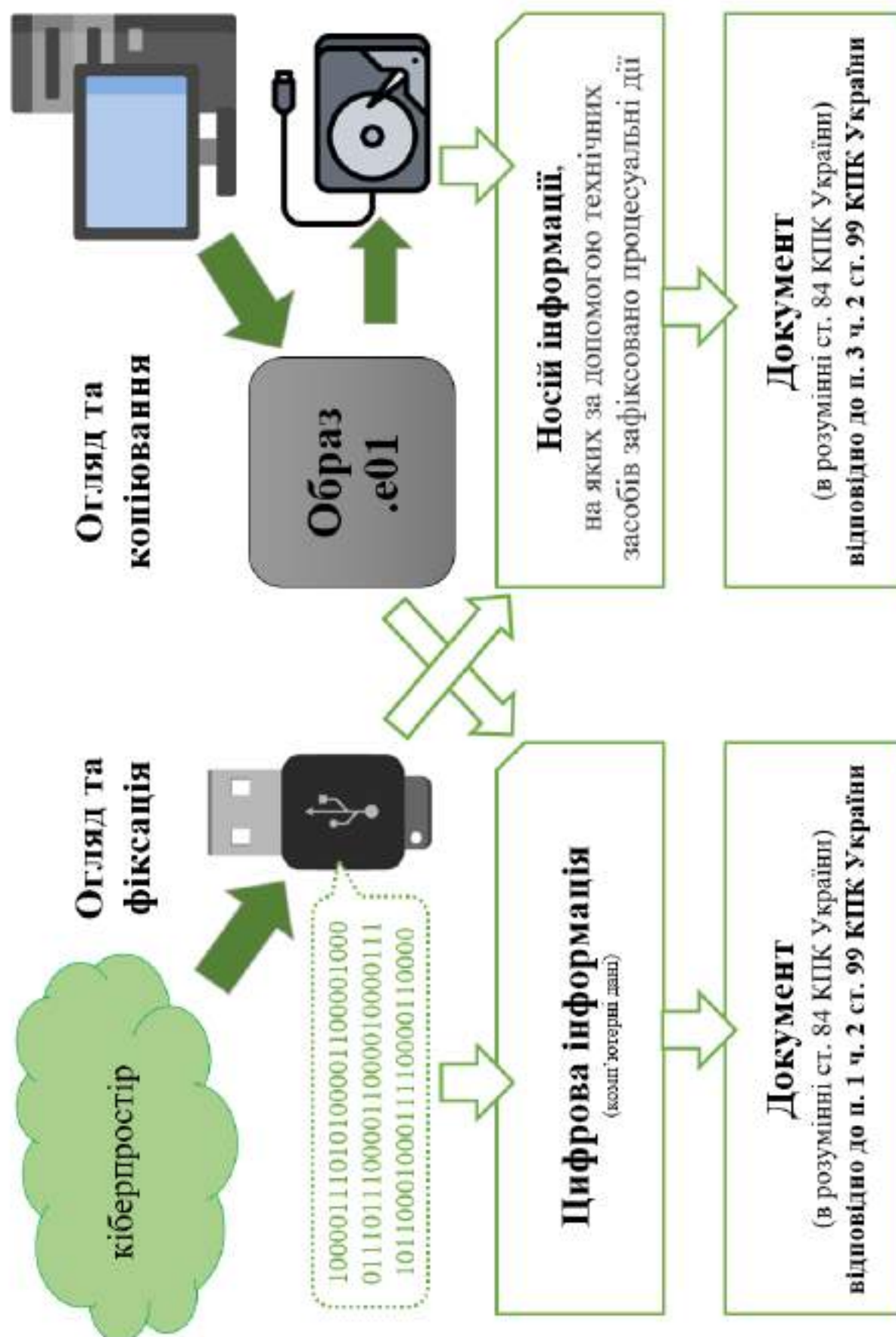
Рис. 16. Дані щодо оптимальної форми отримання знань про докази, що мають електронну форму

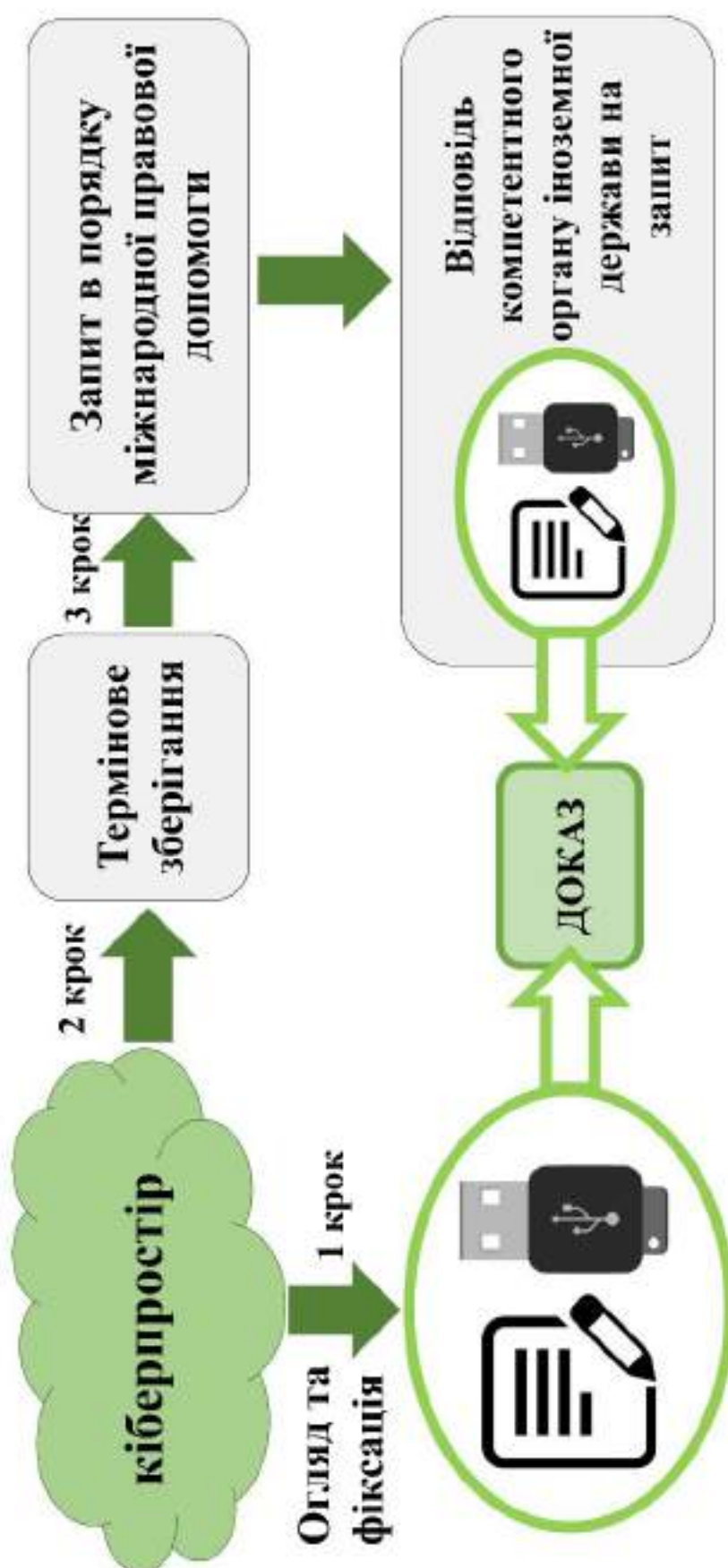




Фізичне вилучення







ПРОПОЗИЦІЇ ЩОДО ОФОРМЛЕННЯ ПРОТОКОЛУ ОГЛЯДУ КІБЕРПРОСТОРУ

*курсивом – примітки та пояснення автора, що не є структурно складовою
бланку процесуального документа*

ПРОТОКОЛ ОГЛЯДУ

місто _____

«___» _____ 20__ року

Огляд розпочато о «___» год. «___» хв.

Огляд закінчено о «___» год. «___» хв.

(посада прокурора, ППБ)

здійснюючи нагляд за додержанням законів під час проведення досудового розслідування у формі процесуального керівництва досудовим розслідуванням

кримінального провадження № _____ від
____.____.____ за ознакам кримінального правопорушення передбаченого
_____ КК України, відповідно до ст.ст. 36, 93, 104-107, 223, 237 КПК України,
провів огляд електронного ресурсу.

Під час огляду використовувалися технічні засоби: комп'ютер на базі процесора _____ (Наприклад: Intel (R) Atom (TM) CPU Z3775 1,46 Ghz) з операційною системою _____ (Наприклад: Windows 10 Home), принтер _____ (Наприклад: Canon LBP6030w).

Об'єктом огляду є _____.

За допомогою додатку _____ (Наприклад: Telegram Desktop) здійснено пошук зазначеного повідомлення/публікації у «_____» з назвою «_____» (російською мовою «_____»), який розміщений за посиланням «_____». В описі до каналу зазначено, що це «_____» (російською мовою «_____»).

У публікаціях (повідомленнях) від _____.____._____ виявлено повідомлення/публікацію наступного змісту:

«_____»

_____».

(зміст/ опис повідомлення/публікації)

Зазначене повідомлення опубліковане _____.____._____ о ____ год. ____ хв.

З метою збереження змісту веб-сторінки виготовлено _____ зображень екрану (скріншотів).

Виготовлені зображення екрану (скріншоти) роздруковано на _____ арк., засвідчені підписом прокурора та додаються до протоколу.

Виготовлені зображення екрану (скріншоти) скопійовано до папки «додаток до протоколу огляду від _____.____.2022», яка створена на флеш-носії _____ (Наприклад, *Transcend 8Gb Micro SDHC*), який долучається до протоколу.

Після зазначеного повідомлення опубліковано відеозапис тривалістю _____ хв. _____ сек., який під час огляду було завантажено на комп'ютер. Відеозапис має назву «_____», тип файлу «_____», розмір файлу _____ МБ.

Завантажений відеозапис скопійовано до папки «додаток до протоколу огляду від _____.____.2022», яка попередньо створена на флеш-носії _____ (Наприклад, *Transcend 8Gb Micro SDHC*), який долучається до протоколу.

За допомогою Інтернет-браузера _____ (Наприклад: *Google Chrome*) (версія _____ (Наприклад: 98.0.4758.102)) відкрито веб-сайт за адресою <https://www.metadata2go.com/>, куди завантажено указаний відеозапис та проведено його аналіз з метою отримання всіх наявних у файлі метаданих. Звіт аналізу було розміщено за посиланням https://_____.

Звіт аналізу, який розміщено за вказаним посиланням роздруковано на _____ аркушах, засвідчені підписом прокурора та додаються до протоколу.

З метою збереження веб-сторінки з результатами аналізу (звітом) здійснено її архівацію за допомогою Інтернет-ресурсу <https://archive.ph>, де у графі «Архівувати сторінку, яка зараз онлайн» (російською мовою «Архивировать страницу, которая сейчас онлайн») введено Інтернет адресу: https://_____, та запущено процес архівації шляхом натискання кнопки «зберегти» (російською мовою «сохранить»).

Після завершення архівації при натисканні вкладки поділитися (російською мовою «поделиться») на сторінці з'являється наступна інформація, що містить посилання на адреси збереженої сторінки та інші відомості.

Збережена сторінка в архіві доступна за наступними посиланнями:
http://_____ (коротке) та
http://_____
 (повне).

Веб-сторінку архівовано, завантажено, скопійовано до папки «додаток до протоколу огляду від _____.____.2022», яка попередньо створена

на флеш-носії _____ (Наприклад, *Transcend 8Gb Micro SDHC*), який долучається до протоколу.

На цьому слідчу дію завершено.

Додатки до протоколу огляду:

1) Зображення (скріншот(и)) на ____ арк.

2) Звіт аналізу на ____ арк.

3) Флеш-носій _____ об'ємом «____» ГБ

№ _____ на якому зафіксовано ____ електронних файлів:

- зображення (скріншот(и)) «_____» у форматі «_____», розміром _____ КБ;

- відеозапис «_____» у форматі «_____», розміром _____ КБ;

- веб-сторінка «_____» у форматі «_____», розміром _____ КБ;

загальним обсягом «_____» КБ.

(посада прокурора)

(ПІБ прокурора)

**Міжвідомча інструкції
про порядок взаємодії органів досудового розслідування та органів
прокуратури з Національним контактним пунктом 24/7, що функціонує
відповідно до статті 35 Конвенції про кіберзлочинність**

I. Загальні положення

1.1. Ця Інструкція визначає механізм організації взаємодії органів досудового розслідування й органів прокуратури з Національним контактним пунктом, створеним відповідно до статті 35 Конвенції про кіберзлочинність (далі – НКП 24/7), з метою забезпечення оперативного обміну інформацією, координації дій та використання процедур міжнародної співпраці при розслідуванні кримінальних правопорушень, учинених з використанням інформаційно-телекомунікаційних систем.

1.2. НКП 24/7 в Україні функціонує в структурі Департаменту кіберполіції Національної поліції України.

1.3. НКП 24/7 здійснює приймання, розгляд та виконання термінових запитів, пов'язаних з реалізацією процедур оперативної координації відповідно до статті 35 Конвенції про кіберзлочинність.

1.4. Взаємодія, передбачена цією Інструкцією, здійснюється з дотриманням вимог Кримінального процесуального кодексу України, законодавства у сфері захисту інформації та персональних даних, а також з урахуванням міжнародних зобов'язань України.

1.5. Органи досудового розслідування та органи прокуратури України забезпечують належне документування звернень до НКП 24/7 та фіксацію результатів взаємодії задля забезпечення їх подальшого використання у кримінальних провадженнях.

II. Основні принципи та завдання взаємодії.

2.1. Взаємодія організовується на таких принципах:

- оперативності та безперервності обміну інформацією, включно з можливістю направлення термінових запитів цілодобово;
- достовірності та повноти інформації, що передається НКП 24/7;
- офіційності та підконтрольності дій, що передбачає ухвалення процесуальних рішень виключно уповноваженими суб'єктами;
- конфіденційності та захищеності інформації, включно з даними, що можуть мати обмежений доступ;
- недопущення дублювання запитів та несанкціонованого звернення до іноземних партнерів поза межами процедур, визначених міжнародними договорами України.

2.2. Основними завданнями взаємодії є:

- забезпечення швидкої комунікації між українськими компетентними органами та іноземними контактними пунктами 24/7;
- забезпечення можливості негайного збереження даних, що можуть бути втрачені або змінені;
- сприяння ініціюванню процедур міжнародної правової допомоги;
- координація дій щодо встановлення користувачів, технічних параметрів мережевої активності, джерел атак та інших відомостей, важливих для розслідування;
- надання органам досудового розслідування та органам прокуратури інформаційної підтримки щодо реалізації механізмів Конвенції про кіберзлочинність.

III. Порядок направлення та розгляду запитів до НКП 24/7.

3.1. Запити до НКП 24/7 можуть направляти:

- керівник органу досудового розслідування;
- слідчий, який здійснює досудове розслідування кримінального провадження а також особи, що діють відповідно до його доручень, наданих в порядку, визначеному КПК України;
- керівник органу прокуратури;
- прокурор, який здійснює процесуальне керівництво досудовим розслідуванням у кримінальному провадженні а також особи, що діють відповідно до його доручень, наданих в порядку, визначеному КПК України.

3.2. Запит має містити:

- чіткий опис події та кримінального правопорушення;
- правові підстави звернення з посиланням на відповідні положення Конвенції про кіберзлочинність та КПК України;
- конкретний перелік інформації, що потребує збереження або з'ясування;
- підтвердження, що інформація необхідна для розслідування у межах кримінального провадження;
- відомості про уповноважену посадову особу та контактні дані для зворотного зв'язку.

3.3. НКП 24/7 здійснює первинну обробку запиту, у тому числі:

- перевірку формальних вимог;
- визначення терміновості та обсягу можливих заходів;
- установлення наявності підстав для комунікації з іноземним контактним пунктом.

3.4. Інформація, отримана НКП 24/7 від іноземних держав, негайно передається ініціатору запиту та відповідальному прокурору, з дотриманням належного режиму доступу до інформації.

IV. Обов'язок ініціатора запиту щодо подальшого витребування або припинення збереження даних.

4.1. У разі використання механізму термінового збереження даних, передбаченого статтею 16,17 Конвенції про кіберзлочинність, посадова особа, яка ініціювала направлення запиту до НКП 24/7, зобов'язана в найкоротший строк направити запит про міжнародну правову допомогу для витребування

збережених даних у порядку, визначеному КПК України та міжнародними договорами України.

4.2. Уповноважена особа, яка ініціювала направлення запиту до НКП 24/7 зобов'язана забезпечити:

- підготовку та скерування відповідного запиту про міжнародну правову допомогу через Офіс Генерального прокурора або Міністерство юстиції України;

- контроль за дотриманням процесуальних строків, необхідних для збереження правової сили тимчасового заходу;

- інформування НКП 24/7 про направлення запиту, із зазначенням дати та офіційних реквізитів.

4.3. Якщо за результатами вивчення матеріалів кримінального провадження встановлено відсутність потреби у подальшому зберіганні даних, які збережено в іноземній юрисдикції згідно статей 16, 17 Конвенції про кіберзлочинність, ініціатор запиту зобов'язаний невідкладно письмово поінформувати НКП 24/7 для передачі відповідного повідомлення до іноземного контактного пункту 24/7.

4.4. Невиконання обов'язку щодо своєчасного направлення запиту про міжнародну правову допомогу може призвести до втрати доступу до даних та покладає на ініціатора відповідальність за порушення процедури міжнародної взаємодії.

V. Документування та зберігання матеріалів взаємодії.

5.1. Вся кореспонденція з НКП 24/7, отримані чи направлені матеріали, службові документи, протоколи та інші дані фіксуються та зберігаються у матеріалах кримінального провадження відповідно до вимог КПК України.

5.2. У разі здійснення заходів забезпечення інформаційної безпеки або використання спеціальних технічних засобів фіксація та зберігання даних здійснюється відповідно до вимог законодавства України у сфері захисту інформації.

VI. Заключні положення.

6.1. Органи досудового розслідування та органи прокуратури вживають заходів щодо регулярного підвищення кваліфікації працівників, які здійснюють взаємодію з НКП 24/7, зокрема шляхом систематичного навчання, підвищення кваліфікації та обміну досвідом.

6.2. Контроль за дотриманням цієї Інструкції здійснюють керівники відповідних органів у межах їх компетенції.

Додаток И

Бланк

«Оцінка прокурором доказу електронної форми під час погодження процесуальних документів»

Цей технічний документ допоможе прокурору оцінити доказ електронної форми за визначеними критеріями, використовуючи позначки для зручності.

Відповіді, що підкреслено можна оцінювати як такі, що свідчать про дотримання відповідного аспекту при роботі з доказом електронної форми

I. Процесуальний аспект

У цьому розділі прокурору доцільно оцінити чи отримано доказ електронної форми з дотриманням вимог Кримінального процесуального кодексу України.

1.1. Отримання уповноваженою особою:

Слідчого/дізнавача включено до складу групи слідчих/дізнавачів:

☐ Так (п. 1 ч. 2 ст. 39, п. 1 ч. 2 ст. 39-1 КПК України)

☐ Ні

☐ Невідомо

Прокурора включено до групи прокурорів:

☐ Так (ч. 1 ст. 37 КПК України)

☐ Ні

☐ Невідомо

Оперативному працівнику надано доручення:

☐ Так (ч. 1 ст. 41 КПК України)

☐ Ні

☐ Не застосовується (у випадку якщо слідчі (розшукові) дії не здійснювались оперативними працівниками)

☐ Невідомо

1.2. Належна процесуальна підстава / умова / обстановка:

Наявність відповідного процесуального документу (ухвала суду, постанова прокурора тощо) або наступна реалізація належних процесуальних процедур у випадку проведення невідкладного обшуку:

☐ Так, є належна процесуальна підстава, визначена КПК України

☐ Ні, відсутня належна процесуальна підстава або є порушення

☐ Невідомо

Накладення арешту на тимчасово вилучене майно:

☐ Так, арешт накладено належним чином (ст.ст. 167-175 КК України)

☐ Ні, арешт не накладено або є порушення

☐ Не застосовується (у випадку якщо майно повернуто законному володільцю)

☐ Невідомо

1.3. Дотримання встановленої законом процедури:

Застосування відеозапису:

☐ Так, відеозапис застосовано та він відповідає вимогам (абз. 3 ч. 2 ст. 104, п. 3 ч. 2 ст. 105, ч. 7 ст. 223 КПК України)

☐ Ні, відеозапис не застосовано, хоча це було необхідно

☐ Відеозапис застосовано, але є недоліки (наприклад, неповний, низька якість)

☐ Не застосовується (не вимагається КПК України)

Залучення понять:

☐ Так, понять залучено належним чином (ч. 7 ст. 223 КПК України)

☐ Ні, понять не залучено, хоча це було необхідно

☐ Понять залучено, але є сумніви щодо їхньої об'єктивності або належності залучення

☐ Не застосовується (не вимагалось законом – абз. 3 п. 1 ч. 1 ст. 615 КПК України)

Спосіб ідентифікації комп'ютерних даних (наприклад, гешування):

☐ Так, ідентифікація проведена належним чином, із застосуванням гешування (п. 3 ч. 3 ст. 104 КПК України, п. 5.4.4. ДСТУ ISO/IEC 27037:2017)

☐ Так, ідентифікація проведена іншим належним чином (п. 3 ч. 3 ст. 104 КПК України,)

☐ Ні, спосіб ідентифікації не застосовувався або застосований неналежно

☐ Невідомо

1.4. Залучення спеціаліста для забезпечення безпосередньої технічної допомоги:

Чи відображено в протоколі залучення спеціаліста:

☐ Так (абз. 4 п. 1 ч. 3 ст. 104 КПК України)

☐ Ні

☐ Спеціаліст не залучався (не вимагається КПК України або не здійснювалося здобуття доказів у контексті дотримання вимог ч. 4 ст. 99 КПК України)

Відомості про спеціаліста:

☐ Наявні та повні (абз. 4 п. 1 ч. 3 ст. 104 КПК України)

☐ Наявні, але неповні

☐ Відсутні

Наявність освіти спеціаліста:

☐ Підтверджено володіння спеціальними знаннями та навичками в частині наявності освіти, кваліфікації, стажу роботи тощо (ч. 1 ст. 71 КПК України)

☐ Не підтверджено володіння спеціальними знаннями та навичками

☐ Невідомо

Наявність сертифікації програмних засобів, що використовувались спеціалістом:

☐ Так, сертифікація підтверджена

- ☐ Ні, сертифікація відсутня або не підтверджена
- ☐ Не застосовується (програмні засоби не потребували сертифікації)
- ☐ Невідомо

Наявність сертифікації технічних засобів, що використовувались спеціалістом:

- ☐ Так, сертифікація підтверджена
- ☐ Ні, сертифікація відсутня або не підтверджена
- ☐ Не застосовується (технічні засоби не потребували сертифікації)
- ☐ Невідомо

1.5. Застосування спеціалістом технічних засобів, пояснення процесів, надані консультації:

Чи відображено в протоколі факт застосування спеціалістом технічних засобів:

- ☐ Так (абз. 1 ч. 2 ст. 104 КПК України)
- ☐ Ні
- ☐ Невідомо

Чи наявні в матеріалах кримінального провадження пояснення процесів, надані консультації – усні чи письмові:

- ☐ Так, є письмові пояснення/консультації в матеріалах провадження (п. 2 ч. 2 ст. 105 КПК України)
- ☐ Так, є усні пояснення/консультації, відображені в протоколі (абз. 5 п. 3 ч. 3 ст. 104 КПК України)
- ☐ Ні, пояснення/консультації відсутні або не зафіксовані
- ☐ Невідомо

II. Технічний аспект

У цьому розділі прокурору доцільно оцінити цілісність інформації, що є доказом та електронного носія інформації на якому він зберігається

2.1. Наявність носія інформації:

Кількість носіїв:

- ☐ Відповідає опису в протоколі
- ☐ Не відповідає
- ☐ Невідомо

Опис носія:

- ☐ Відповідає опису в протоколі, є детальний опис
- ☐ Не відповідає опису або опис неповний/відсутній

2.2. Належне упакування носія інформації:

Відповідність пакування опису в протоколі:

- ☐ Так, пакування відповідає опису
- ☐ Ні, пакування не відповідає або опис відсутній

Цілісність пакування:

- ☐ Так, пакування цілісне, без пошкоджень
- ☐ Ні, пакування пошкоджене або його цілісність порушена
- ☐ Невідомо

2.3. Правильне маркування носія інформації:

Відповідність маркування опису в протоколі:

- ☐ Так, маркування чітке і відповідає опису
- ☐ Ні, маркування відсутнє, нечітке або не відповідає опису
- ☐ Невідомо

2.4. Наявність резервної копії (виготовленої в порядку ч. 4 ст. 99 КПК України, що визнаватиметься судом як оригінал документу):

☐ Так, є належним чином виготовлена резервна копія, що відповідає ч. 4 ст. 99 КПК України

- ☐ Ні, резервна копія відсутня
- ☐ Резервна копія є, але її відповідність ч. 4 ст. 99 КПК України під сумнівом (наприклад, відсутній належний протокол виготовлення)
- ☐ Не застосовується (резервна копія не створювалася)
- ☐ Невідомо

2.5. Перевірка геш-суми:

- ☐ Так, геш-сума перевірена і збігається
- ☐ Ні, геш-сума не перевірялася
- ☐ Геш-сума перевірена, але не збігається
- ☐ Невідомо

ЗАКОН УКРАЇНИ**Про внесення змін та доповнень до Кримінального процесуального кодексу України щодо врегулювання роботи з доказами електронної форми під час кримінального провадження**

Верховна Рада України п о с т а н о в л я є:

I. Внести до Кримінального процесуального кодексу України (Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88, із подальшими змінами) такі зміни:

1. Частину 1 статті 3 пропонується доповнити підпунктами 29-37 наступного змісту:

«29) дані про рух інформації – це відомості, що відображають факт, маршрут, спосіб, час, умови, технічні параметри та середовище передавання, обміну, модифікації чи доступу до інформації, включаючи електронні комунікації та цифрові операції.

30) дані, які зберігаються - будь-яка інформація у формі комп'ютерних даних чи в іншій формі, що охоплює такі складові (але не обмежується ними): інформація, скерована на ідентифікацію користувача комунікаційних послуг, за допомогою якої можна встановити тип комунікаційної послуги, яку використовують, її технічні положення і період користування послугою, особистість користувача послуг, поштову або географічну адресу, телефони та інший номер доступу, у тому числі IP-адресу, інформацію про рахунки і платежі, а також будь-яку іншу інформацію про місце встановлення комунікаційного обладнання, включаючи інформацію, яку можна отримати за допомогою угоди або домовленості про постачання послуг (інформація про користувача послуг); будь-які комп'ютерні дані, пов'язані з комунікацією за допомогою комп'ютерної системи, які були створені комп'ютерною системою, що складала частину ланцюга комунікації, і які зазначають походження, кінцевий пункт, маршрут, час, дату, розмір та тривалість комунікації або тип основної послуги (дані про рух інформації); зміст даних комунікації;

31) електронний носій інформації - це пристрій, система або інша технічно-функціональна платформа, що забезпечує запис, обробку, зберігання, передачу чи відображення інформації в електронній формі,

включаючи її цифрове кодування, системне структурування та можливість технічної реконструкції змісту;

32) кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

33) комп'ютерна система - будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних;

34) комп'ютерні дані - будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою;

35) матеріальний носій інформації - це об'єкт фізичного світу, на якому інформація відображена у формі, доступній для її сприйняття, фіксації, вилучення, дослідження та використання як у процесі доказування, так і поза ним. Матеріальний носій має стабільну фізичну структуру, містить інформацію у матеріалізованому вигляді та може бути оглянутий без застосування спеціального програмного забезпечення чи електронних засобів доступу.

36) цілісність інформації - це стан збереження інформації, за якого забезпечено її незмінність, повноту, достовірність та відтворюваність у первісному обсязі та змісті, включно з характеристиками форми представлення та супровідними даними (метаданими), з моменту її створення або фіксації і до використання у процесі доказування, шляхом запобігання несанкціонованому доступу, модифікації, знищенню, спотворенню або підміні.

37) цілісність комп'ютерних даних – це стан збереження комп'ютерних даних, за якого забезпечено їхню незмінність, повноту, достовірність і відтворюваність від моменту виявлення, вилучення чи фіксації до моменту використання в кримінальному провадженні, шляхом унеможливлення несанкціонованого доступу, модифікації, видалення, часткового знищення, підміни або спотворення інформації та пов'язаних з нею метаданих.»;

2. Частину 2 статті 71 пропонується викласти в такій редакції:

«2. Спеціаліст може бути залучений для надання безпосередньої технічної допомоги (фотографування, складення схем, планів, креслень, копіювання комп'ютерних даних, відбір зразків для проведення експертизи тощо) слідчим суддею та сторонами кримінального провадження під час досудового розслідування, судом під час судового розгляду, а також для надання довідок, висновків та інших документів у випадках, передбачених пунктами 7, 8, 9 частини четвертої цієї статті.»;

3. Пункт 9 частини 4 статті 71 пропонується викласти в такій редакції:

«9) надавати довідки, висновки з питань, що належать до сфери його знань, щодо ідентифікації особи, комп'ютерних даних, зброї, бойових припасів, вибухових речовин, вибухових пристроїв, слідів вибуху або пострілу, наркотичних засобів, психотропних речовин, їх аналогів і прекурсорів, сильнодіючих лікарських засобів.»;

4. Частину 2 статті 84 доповнити абзацом другим наступного змісту:

«Докази можуть бути зібрані та представлені як у матеріальній, так і в електронній формі.»;

5. Частину 4 статті 93 доповнити абзацом другим наступного змісту:

«Докази можуть бути одержані також із кіберпростору незалежно від території розташування фізичних носіїв або інформаційної інфраструктури, у якій зберігаються чи обробляються дані, що відображаються як комп'ютерні дані, якщо таке одержання здійснюється у порядку, передбаченому цим Кодексом.»;

6. Доповнити новою статтею 93-1 «Автентичність та цілісність доказів» наступного змісту:

«Стаття 93-1. Автентичність та цілісність доказів

1. Сторони кримінального провадження, слідчий суддя та суд зобов'язані забезпечити, щоб під час одержання, фіксації, передачі, зберігання та дослідження доказів було вжито заходів, спрямованих на недопущення їх зміни, пошкодження, знищення або спотворення.

2. У разі збирання, використання та дослідження доказів електронної форми забезпечується перевірка їх автентичності та цілісності шляхом застосування технічних і процесуальних засобів, зокрема фіксації метаданих, цифрових ідентифікаторів (контрольних сум), журналів дій доступу до даних, а також інших засобів верифікації та підтвердження автентичності та незмінності інформації.

3. Особи, які збирають докази, зобов'язані забезпечити можливість подальшої перевірки їх походження, способу одержання, технічних параметрів та засобів забезпечення цілісності. Відмова від застосування технічних способів забезпечення цілісності доказів електронної форми допускається лише у випадках, коли такі способи є об'єктивно неможливими, з документуванням відповідним підстав та обставин.

4. Докази, щодо яких існують обґрунтовані сумніви в їх автентичності або цілісності, підлягають перевірці, а у разі встановлення втручання, спотворення або порушення способу їх одержання та зберігання, що вплинуло на достовірність відомостей, можуть бути визнані недопустимими.»;

7. Статтю 94 доповнити частиною третьою наступного змісту:

«3. Цілісність доказів, отриманих або поданих в електронній формі (комп'ютерних даних, електронних документів тощо), має бути підтверджена технічними засобами або способами, що забезпечують перевірку їх автентичності та незмінності.»;

8. Доповнити новою статтею 94-1 «Ланцюг збереження доказів електронної форми» наступного змісту:

«Стаття 94-1. Ланцюг збереження доказів електронної форми

1. Ланцюг збереження доказів (chain of custody) електронної форми є сукупністю документально підтверджених дій, спрямованих на забезпечення автентичності, цілісності та простежуваності походження доказів електронної форми від моменту їх одержання до завершення кримінального провадження.

2. Під час збирання, фіксації, передачі, зберігання, дослідження та використання доказів електронної форми забезпечується ведення ланцюга збереження таких доказів, який повинен містити:

- 1) унікальний ідентифікатор доказу;
- 2) зафіксовану хронологію дій з таким доказом, включаючи кожен операцію доступу, копіювання, переміщення, передачі та дослідження;
- 3) фіксацію осіб, відповідальних за виконання кожної зареєстрованої дії, із зазначенням дати, часу, технічних засобів та мети доступу;
- 4) створення щонайменше двох резервних копій доказів електронної форми, що зберігаються окремо одна від одної, із забезпеченням їх захисту від змін;
- 5) застосування засобів контролю доступу до доказів електронної форми, включаючи журнал доступів та технічні засоби автентифікації;
- 6) фіксацію цифрових ідентифікаторів (контрольних сум) для первинних електронних даних та їх копій із забезпеченням можливості незалежної верифікації таких цифрових ідентифікаторів (контрольних сум) сторонами кримінального провадження, спеціалістом або експертом.

3. Порушення вимог, визначених у частині другій цієї статті, не є безумовною підставою для визнання доказів електронної форми недопустимими, якщо таке порушення не вплинуло на їх достовірність та можливість перевірки їх автентичності і цілісності.

4. З метою додаткового забезпечення автентичності та цілісності доказів електронної форми допускається використання реєстрів незмінних міток, у тому числі створених на базі розподіленого реєстру (distributed ledger technology), як факультативного механізму фіксації ланцюга збереження доказів та підтвердження незмінності даних.»;

9. Частину 1 статті 95 викласти в такій редакції:

«1. Показання - це відомості, які надаються в усній або письмовій формі під час допиту підозрюваним, обвинуваченим, свідком, потерпілим, експертом

щодо відомих їм обставин у кримінальному провадженні, що мають значення для цього кримінального провадження, у тому числі проведеного в режимі відеоконференції з використанням електронних засобів телекомунікації.»;

10. В частині 1 статті 99 виключити слова «матеріальний»;

11. Частину 4 статті 99 викласти в такій редакції:

«4. Дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), визнається судом як оригінал документа.

Копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із забезпеченням підтвердження цілісності комп'ютерних даних, визнаються судом як оригінал документа.»;

12. Частину 7 статті 101 викласти в такій редакції:

«7. Висновок експерта надається в письмовій формі, що включає як матеріальну форму висновку, підписаного власноручним підписом експерта, так і електронну форму висновку, оформлену як електронний документ та підписану кваліфікованим електронним підписом експерта відповідно до закону № 851-IV.

Кожна сторона має право звернутися до суду з клопотанням про виклик експерта для допиту під час судового розгляду для роз'яснення чи доповнення його висновку.»;

13. Частину 3 статті 102 викласти в такій редакції:

«3. Якщо при проведенні експертизи будуть виявлені відомості, які мають значення для кримінального провадження і з приводу яких не ставилися питання, експерт має право зазначити про них у своєму висновку.

Висновок підписується експертом власноручним підписом у разі його складення в матеріальній формі або кваліфікованим електронним підписом експерта у випадку складення висновку у формі електронного документа відповідно до закону № 851-IV.»;

14. Доповнити новою статтею 100-1 «Зберігання доказів електронної форми» наступного змісту:

«Стаття 100-1. Зберігання доказів електронної форми

1. Докази електронної форми та електронні носії інформації, на яких вони містяться, підлягають зберіганню у порядку, що забезпечує їх автентичність, цілісність, доступність для сторін кримінального провадження, захист від модифікації, пошкодження, знищення, блокування доступу, а також гарантує дотримання ланцюга зберігання доказів (chain of custody).

2. Зберігання доказів електронної форми може здійснюватися:

1) шляхом зберігання оригінальних електронних носіїв інформації;

2) шляхом зберігання ідентичних копій (бітових образів) відповідних електронних носіїв інформації;

3) у інформаційній системі зберігання доказів електронної форми, що функціонує відповідно до вимог інформаційної безпеки, захисту персональних даних та електронних доказів;

4) у Інформаційно-комунікаційній системі досудового розслідування.

3. Під час передачі, зберігання та доступу до доказів електронної форми забезпечується визначення цифрових ідентифікаторів (контрольних сум) таких доказів та їх копій. Значення цифрових ідентифікаторів (контрольних сум) фіксуються в протоколі, актах приймання-передачі та інших процесуальних документах.

4. Будь-яке отримання доступу до доказів електронної форми або їх технічна обробка здійснюється з обов'язковою автоматизованою фіксацією журналу доступу, що містить відомості про дату, час, суб'єкта доступу, підстави доступу, вид доступу та зміни, якщо такі мали місце.

5. Зберігання оригінальних електронних носіїв інформації здійснюється у спеціально обладнаних приміщеннях або сейфах, що забезпечують фізичну безпеку таких носіїв інформації та запобігають їх пошкодженню.

6. У разі, якщо вилучення комп'ютерної системи або її частини, електронного носія інформації може призвести до припинення або істотного обмеження діяльності органу державної влади, об'єкта критичної інфраструктури або суб'єкта господарювання, зберігання доказів електронної форми здійснюється шляхом створення бітової копії (образу) з визначенням цифрових ідентифікаторів (контрольних сум) електронних даних, а оригінальний носій залишається у володільця, якщо інше не обумовлено необхідністю проведення судової експертизи або не суперечить вимогам інформаційної безпеки.

7. Сторони кримінального провадження мають право на доступ до доказів електронної форми, отримання їх копій або витягів, а також на проведення перевірки цілісності та автентичності таких доказів за допомогою цифрових ідентифікаторів (контрольних сум) у порядку, визначеному цим Кодексом.

8. Порядок функціонування інформаційній системі зберігання доказів електронної форми, вимоги до технічного та криптографічного захисту, форматів даних, визначення цифрових ідентифікаторів (контрольних сум), ведення журналів доступу, а також порядок взаємодії з органами досудового розслідування, прокурорами та судами визначаються Кабінетом Міністрів України.»;

15. Статтю 104 доповнити частинами 7-9 наступного змісту:

«7. Протокол процесуальної дії, проведеної у режимі відеоконференції, може складатися в електронній формі та підписуватися кваліфікованими

електронними підписами учасників процесуальної дії. Відеозапис процесуальної дії є невід'ємним додатком до такого протоколу.

8. Протокол, складений в електронній формі, повинен містити метадані створення, відомості про використаний засіб електронного підпису, а також автоматично фіксувати журнал доступу до нього у цифровому архіві кримінального провадження. До такого протоколу обов'язково долучається машинозчитуваний технічний додаток, що містить перелік файлів, їх контрольні суми, технічні метадані та журнал дій.

9. У разі здійснення зняття показань технічних приладів або зняття інформації з технічних засобів, що мають функції фото-, кіно-, відеозапису, складається протокол відповідно до вимог цього Кодексу. До протоколу включаються опис технічного засобу та умов доступу до нього, технічні параметри отриманих даних, застосовані засоби забезпечення цілісності та автентичності електронних даних, у тому числі цифрові ідентифікатори (контрольні суми) електронних даних, а також відомості про програмні й апаратні засоби, використані під час доступу та копіювання даних. Відеозапис або інші електронні дані долучаються у вигляді машинозчитуваного технічного додатка, що містить метадані, перелік файлів, контрольні суми та журнал дій щодо доступу до даних.»;

16. В пункті 4 частини 2 статті 105 слова «носії комп'ютерних даних» замінити на «електронні носії інформації»;

17. Частину 2 статті 105 доповнити пунктом 5 наступного змісту:

«5) машинозчитуваний технічний додаток, що містить метадані, технічні параметри отриманих електронних даних, цифрові ідентифікатори (контрольні суми) електронних даних, журнал дій та інші технічні відомості, необхідні для перевірки автентичності та цілісності електронних даних.»;

18. Частину 1 статті 107 доповнити абзацом наступного змісту:

«При проведенні процесуальних дій, пов'язаних із доступом до електронних інформаційних систем, електронних носіїв інформації або телекомунікаційних мереж, допускається застосування запису екрану, фіксації мережевого трафіку, журналювання системного часу та фіксації часових міток відповідних операцій.»;

19. Частину 3 статті 107 викласти в такій редакції:

«3. У матеріалах кримінального провадження зберігаються примірники електронних носіїв інформації зафіксованої процесуальної дії, резервні копії яких зберігаються окремо. Фіксування за допомогою технічних засобів кримінального провадження під час розгляду питань слідчим суддею та в суді під час судового провадження здійснюється в порядку, передбаченому частиною четвертою цієї статті.

Електронні записи, отримані у результаті застосування запис екрану, фіксація мережевого трафіку або інших електронних способів фіксації

взаємодії з електронними об'єктами, зберігаються як електронні додатки до протоколу з обов'язковим зазначенням цифрових ідентифікаторів (контрольних сум) та метаданих запису.»;

20. Частину 4 статті 107 доповнити абзацом наступного змісту:

«У разі застосування технічних засобів фіксації дій з електронними інформаційними системами або електронними носіями інформації, відеозапис, запис екрану, фіксація мережевого трафіку та інші електронні записи є невід'ємним додатком до протоколу і повинні містити фіксацію системного часу та часових міток, що забезпечують реконструкцію дій учасників процесуальної дії.»;

21. Частину 6 статті 107 доповнити абзацом наступного змісту:

«Записи, зазначені у частинах першій та третій цієї статті, підлягають збереженню в електронній формі з обов'язковим визначенням цифрових ідентифікаторів (контрольних сум), фіксацією метаданих та журналюванням доступу до них у порядку статті 100-1 цього Кодексу.»;

22. Частину 2 статті 131 доповнити пунктом 5-1 наступного змісту:

«5⁻¹) термінове збереження комп'ютерних даних, що зберігаються;»;

23. Частину 1 статті 159 викласти в такій редакції:

«1. Тимчасовий доступ до речей і документів полягає у наданні стороні кримінального провадження особою, у володінні якої знаходяться такі речі і документи, можливості ознайомитися з ними, зробити їх копії та вилучити їх (здійснити їх виїмку).

Тимчасовий доступ до електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах, комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення, окрім випадків якщо виготовлення копії такої інформації технічно неможливе.

Забороняється вилучення (виїмка) матеріальних та електронних носіїв інформації, пов'язаних із веденням Центральним депозитарієм цінних паперів та депозитарними установами системи депозитарного обліку цінних паперів, облікової системи часток товариств з обмеженою відповідальністю та товариств з додатковою відповідальністю (далі - облікова система часток) і внесенням змін до них.»;

24. Статтю 160 доповнити частинами 3 та 4 наступного змісту:

«3. За клопотанням прокурора суд має право постановити ухвалу, якою зобов'язати:

1) будь-яку особу надати комп'ютерні дані, якими така особа володіє або які контролює і які зберігаються у комп'ютерній системі або на електронному носії інформації;

2) постачальника послуг, який пропонує свої послуги на території України, надавати інформацію про користувача послуг, пов'язану із такими послугами, яка перебуває у власності або під контролем такого постачальника послуг.

4. Якщо є підстави вважати, що інформація про користувача послуг може бути втрачена, прокурор може постановити ухвалу якою зобов'язати постачальника послуг надати інформацію про користувача послуг до постановлення ухвали суду, зазначеної в частині 3 цієї статті.»;

25. У частині 1 статті 161 після слів «1. Речами і документами» доповнити словами «, як у матеріальній, так і в електронній формі,»;

26. У частині 1 статті 162 після слів «речей і документів» доповнити словами «, як у матеріальній, так і в електронній формі,»;

27. У частині 1 статті 163 після слів «речей і документів» доповнити словами «, включно з тими, що мають як матеріальну, так і електронну форму, »;

28. Пункт 6 частини 1 статті 164 доповнити абзацом наступного змісту:

«У випадках, коли документи існують в електронній формі, слідчий суддя може постановити ухвалу про вилучення комп'ютерних систем або їх частин, що містять необхідну інформацію, лише за умови, коли отримання точної копії електронної інформації буде технічно неможливим. У всіх інших випадках порядок повинен дозволяти отримання точної копії витребовуваних електронних даних;»;

29. Статтю 165 викласти в такій редакції:

«Стаття 165. Виконання ухвали слідчого судді, суду про тимчасовий доступ до речей і документів

1. Особа, яка зазначена в ухвалі слідчого судді, суду про тимчасовий доступ до речей і документів як володілець речей або документів, зобов'язана надати тимчасовий доступ до зазначених в ухвалі речей і документів, у матеріальній або електронній формі, особі, зазначеній у відповідній ухвалі слідчого судді, суду.

2. Зазначена в ухвалі слідчого судді, суду особа зобов'язана пред'явити особі, яка зазначена в ухвалі як володілець речей і документів, оригінал ухвали про тимчасовий доступ до речей і документів та вручити її копію. Ухвала про тимчасовий доступ до речей може бути пред'явлена в електронній формі.

3. Особа, яка пред'являє ухвалу про тимчасовий доступ до речей і оригіналів або копій документів, зобов'язана залишити володільцю речей і оригіналів або копій документів, копій комп'ютерних даних, опис речей і оригіналів або копій документів, які були вилучені на виконання ухвали слідчого судді, суду.

4. На вимогу володільця особою, яка пред'являє ухвалу про тимчасовий доступ до речей і документів, має бути залишено копію вилучених оригіналів

документів, копій комп'ютерних даних у випадку вилучення комп'ютерних систем або їх частин. Копії документів, копій комп'ютерних даних, які вилучаються або оригінали яких вилучаються, виготовляються з використанням копіювальної техніки, електронних засобів володільця (за його згодою) або копіювальної техніки, електронних засобів особи, яка пред'являє ухвалу про тимчасовий доступ до речей і документів.»;

30. Доповнити новою статтею 166-1 «Термінове збереження комп'ютерних даних, що зберігаються та тимчасове розкриття даних про рух інформації» наступного змісту:

«Стаття 166-1. Термінове збереження комп'ютерних даних, які зберігаються та тимчасове розкриття даних про рух інформації

1. Якщо існують підстави вважати, що комп'ютерні дані, що зберігаються, можуть бути втрачені чи модифіковані, слідчий або прокурор має право зобов'язати будь-яку фізичну чи юридичну особу, яка володіє такими даними або під чиїм контролем ці дані обґрунтовано можуть перебувати, а також будь-яку іншу особу, що має стосунок до справи, зберігати такі комп'ютерні дані та забезпечувати їхню цілісність упродовж 90 днів. За потреби цей термін може бути продовжено ще на 90 днів.

2. У контексті цілей цієї статті комп'ютерні

3. Особа, яка повинна зберігати комп'ютерні дані, зобов'язана зберігати конфіденційність факту проведення таких процедур упродовж періоду, визначеного частиною 1 цієї статті.

4. У випадку визначеному ч. 3 ст. 264-1 цього Кодексу, слідчий або прокурор у постанові про збереження даних може також зобов'язати таку особу негайно розкрити достатню кількість даних про рух інформації на вимогу, для забезпечення визначення постачальника послуг та шляхів, якими здійснювалась комунікація.»;

31. Доповнити новою статтею 168-1 «Збирання та здобуття доказів електронної форми» наступного змісту:

«Стаття 168¹. Збирання та здобуття доказів електронної форми

1. Збиранням доказів електронної форми полягає у фізичному вилученні електронних носіїв інформації, електронних інформаційних систем або їх частин, інших пристроїв чи технічних засобів, що містять такі відомості або забезпечують доступ до них, з метою їх подальшого дослідження та збереження.

2. Здобуттям доказів електронної форми полягає у копіюванні, створенні бітового образу або витягу інформації з електронного носія інформації, електронної інформаційної системи чи телекомунікаційної мережі без обов'язкового фізичного вилучення відповідного носія або технічного засобу, однак не виключає можливості такого вилучення.

3. Здобуття доказів електронної форми застосовується першочергово, якщо це технічно можливо та не створює ризику зміни, втрати або пошкодження доказів. Фізичне вилучення електронних носіїв або технічних засобів допускається у випадках, коли здобуття доказів є технічно неможливим, пов'язане з неприйнятним ризиком для їх цілісності, існує обґрунтований ризик їх модифікації, знищення або приховування, або на інших підставах, передбачених законом.

4. Перед початком збирання або здобуття доказів електронної форми складається протокол відповідної слідчої (розшукової) дії, в якому зазначаються: дата, місце, час початку і закінчення дії, перелік виявлених електронних носіїв та електронних інформаційних систем, їх ідентифікаційні та технічні характеристики, підстави та обґрунтування обраного способу отримання доказів, перелік учасників, відомості про залучення спеціаліста, а також відомості про технічні засоби, що застосовувалися.

5. У разі здобуття доказів електронної форми складається технічний протокол, який містить опис застосованих методів, програмних та апаратних засобів, параметрів копіювання або створення бітового образу, часові позначки відповідних операцій, інформацію про джерело отримання даних та процедуру їх верифікації, а також підписи уповноважених осіб.

6. Для підтвердження цілісності та автентичності інформації, отриманої в порядку цієї статті, здійснюється визначення цифрових ідентифікаторів (контрольних сум) електронних даних. Визначення цифрових ідентифікаторів (контрольних сум) електронних даних проводиться перед отриманням інформації, після створення копії або бітового образу, при передачі носіїв або матеріалів, а також під час їх дослідження. Значення цифрових ідентифікаторів (контрольних сум) електронних даних вносяться до протоколів та технічних матеріалів.

7. У разі зміни цифрових ідентифікаторів (контрольних сум) електронних даних під час їх зберігання або дослідження така обставина фіксується у протоколі із зазначенням можливих причин та повідомленням слідчого або прокурора.

8. Збирання та здобуття доказів електронної форми здійснюється за участю або під наглядом спеціаліста. У разі неможливості його залучення під час проведення відповідної дії слідчий або прокурор забезпечує участь спеціаліста або експерта у подальшій технічній обробці отриманих матеріалів.

9. Отримання інформації з віддалених електронних інформаційних систем, серверів або телекомунікаційних мереж здійснюється в порядку, передбаченому цим Кодексом.

10. Оригінальні електронні носії інформації або технічні засоби після їх вилучення опечатуються та зберігаються відповідно до правил, визначених цим Кодексом, із фіксацією умов їх зберігання та відповідальних осіб.»;

32. Частину 1 статті 170 доповнити абзацом наступного змісту:

«Арешт може накладатися також на облікові записи, доменні імена, електронні кабінети, хмарні сховища, облікові записи у цифрових платформах, віртуальні активи, цифрові токени, криптоактиви та інші нематеріальні носії або об'єкти даних, що мають економічну або доказову цінність.»;

33. Частину 2 статті 170 доповнити пунктом 5 наступного змісту:

«5) забезпечення збережуваності комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, електронних носіїв інформації чи інших технічних засобів/пристроїв, що містять комп'ютерні дані, копіювання яких неможливе без втрати цілісності їх змісту.»;

34. Абзац 2 частини 3 статті 170 доповнити частиною наступного змісту:

«Арешт серверів, дата-центрів, хмарних середовищ зберігання даних, корпоративних інформаційних систем та іншої критичної інформаційної інфраструктури не допускається у разі, якщо для досягнення цілей кримінального провадження є достатнім створення повної та достовірної копії (образу) потрібних даних із забезпеченням їх цілісності. У таких випадках слідчий, прокурор зобов'язаний забезпечити безперервність функціонування відповідних систем, якщо інше не зумовлено безпосередніми потребами кримінального провадження.»;

35. Частину 3 статті 170 доповнити абзацом наступного змісту:

«Забороняється накладати арешт на об'єкти критичної ІТ-інфраструктури, необхідні для забезпечення оборони, безпеки, фінансової стабільності держави, життєво важливих послуг або безперервності господарської діяльності, крім випадків, коли доведено неможливість досягнення цілей кримінального провадження іншим шляхом.»;

36. Статтю 232 доповнити частиною 12 наступного змісту:

«12. Проведення процесуальних дій у режимі відеоконференції допускається як між територіальними підрозділами правоохоронних органів чи судами України, так і з відповідними компетентними органами іноземних держав — у порядку, визначеному міжнародними договорами України або на засадах взаємності.»;

37. Доповнити новою статтею 232-1 «Віддалений міждержавний допит свідка в режимі відеоконференцзв'язку» наступного змісту:

«Стаття 232-1. Віддалений міждержавний допит свідка в режимі відеоконференцзв'язку

1. Віддалений міждержавний допит свідка полягає у наданні свідком показань у режимі відеоконференцзв'язку з території іншої держави на підставі міжнародного запиту про правову допомогу, у випадках та порядку, передбачених міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України, та цим Кодексом.

2. Віддалений міждержавний допит свідка здійснюється за умови забезпечення присутності уповноваженого представника компетентного

органу держави перебування свідка (юрисдикції перебування), відповідального за:

- 1) встановлення особи свідка;
- 2) підтвердження його добровільної участі;
- 3) дотримання гарантій недоторканності та недопущення примусу;
- 4) забезпечення дотримання процесуального порядку;
- 5) засвідчення правильності відображення отриманих свідчень.

3. Перед початком допиту здійснюється:

- 1) перевірка документів свідка, що посвідчують особу;
- 2) ідентифікація свідка шляхом відеофіксації та технічного порівняння біометричних ознак (за наявності технічної можливості);
- 3) фіксація факту перебування свідка на території відповідної іноземної держави;
- 4) роз'яснення прав, обов'язків;
- 5) підтвердження наявності перекладача (у разі необхідності) та посвідчення його особи.

4. Технічне забезпечення віддаленого міждержавного допиту повинно забезпечувати:

- 1) стійкість та безперервність з'єднання;
- 2) можливість ідентифікації учасників у режимі реального часу;
- 3) захист інформації та шифрування комунікації;
- 4) фіксацію технічних параметрів сеансу відеоконференцзв'язку;
- 5) створення відеозапису проведення допиту.

5. За результатами допиту може складатися протокол в електронній формі, який, окрім іншого, повинен містити:

- 1) встановлені дані особи свідка та спосіб ідентифікації;
- 2) посилання на міжнародний запит та підстави правової допомоги;
- 3) відомості про технічні параметри сеансу відеоконференцзв'язку;
- 4) повний текст показань свідка;
- 5) дані представника компетентного органу іноземної держави, перекладача та інших учасників.

Електронний протокол разом із відеозаписом допиту, що є його невід'ємним додатком, засвідчуються засобами, що забезпечують перевірку цілісності інформації.

6. Порушення процедури ідентифікації, відсутність підтвердження юрисдикції перебування або неналежне забезпечення технічних гарантій тягне недопустимість відповідних відомостей як доказів.»;

38. В частині 3 статті 233 після слів «врятуванням життя людей та майна» доповнити словами «, включаючи виявлення та вилучення комп'ютерних даних, що можуть бути знищені або спотворені,»;

39. В пункті 4 частини 5 статті 234 після слів «відшукувані речі, документи» доповнити словами «, в тому числі комп'ютерні дані,»;

40. Пункт 6 частини 2 статті 235 викласти в такій редакції:

«6) речі, документи або осіб, для виявлення яких проводиться обшук. Якщо комп'ютерні дані було виявлено, суддя своєю постановою може визначити, чи є арешт носіїв інформації необхідним, чи зняття копій буде достатньо. Прокурор, слідчий, керуючись обраним суддею методом, контролює виконання постанови, яка включає такі можливі пункти:

арештовувати (забирати) або вчиняти схожі дії щодо комп'ютерної системи чи її частини або комп'ютерного носія інформації;

копіювати і зберігати копії таких комп'ютерних даних;

зберігати цілісність відповідних збережених комп'ютерних даних;

забороняти доступ або вилучення цих комп'ютерних даних із комп'ютерної системи, до якої здійснювався доступ.»;

41. Статтю 236 доповнити частинами 6-1 та 6-2 наступного змісту:

«6-1. Під час доступу до електронних інформаційних систем, носіїв інформації або хмарних ресурсів слідчий, прокурор зобов'язані застосовувати механізми мінімізації втручання у приватність та відбору лише інформації, що має значення для кримінального провадження, зокрема шляхом:

1) пошуку за ключовими словами, часовими межами, ідентифікаторами та іншими релевантними параметрами;

2) використання технічних засобів попереднього фільтрування та огляду даних;

3) попередньої перевірки даних з метою недопущення ознайомлення з комунікаціями, що містять охоронювану законом таємницю, зокрема адвокатську, лікарську, нотаріальну та іншу професійну таємницю;

4) механізмів «відкладеного розкриття» із забезпеченням перевірки слідчим суддею (ex parte) змісту фрагментів, що можуть містити привілейовану інформацію, до надання їх стороні обвинувачення.

6-2. За наявності технічної можливості та якщо це не перешкоджає досягненню мети обшуку, пріоритет має надаватися створенню копії (образу) електронних даних із фіксацією цифрових ідентифікаторів (контрольних сум) електронних даних замість вилучення електронних носіїв чи обладнання.»;

42. Частину 2 статті 237 доповнити абзацами наступного змісту:

«У разі якщо є підстави вважати, що відомості, які необхідно забезпечити для кримінального провадження, існують в електронній формі на комп'ютерній системі або аналогічному пристрої, слідчий, прокурор має

право здійснити тимчасове вилучення комп'ютерної системи, її частини або електронних носіїв інформації для подальшого огляду; створити та зберегти копію відповідних комп'ютерних даних; застосувати технічні заходи для забезпечення цілісності таких даних та запобігання їх зміненню або видаленню; заборонити доступ до відповідних даних або їх вилучення з комп'ютерної системи.

У разі прийняття рішення не про огляд на місці, а про арешт комп'ютерної системи або даних, слідчий, прокурор складає мотивований письмовий звіт про причини такого рішення, який додається до протоколу огляду та оголошується учасникам процесуальної дії. За вимогою учасників огляду слідчий, прокурор надає роз'яснення про можливість здійснення огляду на місці як альтернативи арешту комп'ютерних носіїв та про причини неможливості застосування такої альтернативи. Усі відповідні пояснення та зауваження учасників заносяться до протоколу.»;

43. Частину 5 статті 237 доповнити абзацом наступного змісту:

«Створені копії комп'ютерних даних, здійснені під час огляду, підлягають негайному документуванню, збереженню з використанням цифрових ідентифікаторів (контрольних сум) або іншими технічними засобами забезпечення автентичності та цілісності таких даних, із внесенням відповідних відомостей до протоколу.»;

44. Частину 7 статті 237 доповнити абзацом наступного змісту:

«Огляд комп'ютерних даних і тимчасове вилучення електронного пристрою не є підставою для доступу до інформації, що стосуються приватного листування, що міститься на такому пристрої. Отримання доступу до змісту приватного спілкування особи, у тому числі електронних повідомлень, месенджерів, листування, резервних копій та хмарних акаунтів, допускається лише за наявності окремої ухвали слідчого судді, відповідно до положень цього Кодексу щодо втручання у приватне спілкування.»;

45. Доповнити новою статтею 237-1 «Огляд віртуального середовища (кіберпростору)» наступного змісту:

«Стаття 237-1. Огляд віртуального середовища (кіберпростору)

1. Огляд віртуального середовища (кіберпростору) полягає у фіксації інформації, що міститься у хмарних сервісах, електронних кабінетах, облікових записах, соціальних мережах, месенджерах, інших інформаційних ресурсах або цифрових платформах, доступ до яких отримано у порядку, встановленому цим Кодексом, та які ідентифіковані як такі, що можуть містити відомості, що мають значення для кримінального провадження.

2. Огляд віртуального середовища (кіберпростору) здійснюється з метою документування цифрових даних, їх зовнішнього вигляду, структури, змісту, метаданих та інших характеристик.

3. Під час огляду віртуального середовища забезпечується:

1) фіксація дати, часу (з урахуванням часової зони) та мережевих ідентифікаторів;

2) фіксація адреси ресурсу, ідентифікаторів облікового запису, параметрів авторизації (без розголошення конфіденційних даних);

3) створення скриншотів або іншої візуальної фіксації даних;

4) відеофіксація процесу доступу та огляду (за технічної можливості);

5) збереження копій даних у первинному форматі;

6) обчислення та фіксація цифрових ідентифікаторів (контрольних сум) завантажених матеріалів та метаданих;

7) ведення журналу дій щодо доступу та фіксації даних.

4. Протокол огляду віртуального середовища містить опис програмних засобів, обладнання та налаштувань доступу, технічних параметрів середовища, а також додатки із візуальними матеріалами, файлами та їх ідентифікаторами.

5. Під час огляду можуть застосовуватися міжнародні стандарти документування відомостей з відкритих джерел, що не суперечить цьому Кодексу.»;

46. Доповнити новою статтею 240-1 «Пошук відомостей у віртуальному середовищі (кіберпросторі) на основі відкритих джерел інформації» наступного змісту:

«Стаття 240-1. Пошук відомостей у віртуальному середовищі (кіберпросторі) на основі відкритих джерел інформації

1. Пошук відомостей у віртуальному середовищі (кіберпросторі) на основі відкритих джерел інформації (OSINT) полягає у здійсненні органом досудового розслідування послідовних дій щодо виявлення та фіксації загальнодоступної цифрової інформації, яка може мати значення для кримінального провадження.

2. Пошук відомостей у віртуальному середовищі (кіберпросторі) на основі відкритих джерел інформації включає документування процесу виявлення інформації, логіки переходів між ресурсами, послідовності дій, параметрів середовища та отриманих результатів.

3. Під час пошуку відомостей у віртуальному середовищі (кіберпросторі) на основі відкритих джерел інформації забезпечується:

1) фіксація дати, часу, адрес ресурсів, пошукових запитів, послідовності переходів між веб-сторінками;

2) відеофіксація процесу пошуку або інші способи безперервної фіксації дій;

3) архівне збереження веб-сторінок у формі первинних даних або шляхом фіксації їх змісту;

4) опис програмних інструментів та налаштувань доступу, що використовуються для пошуку за винятком тих, що становлять державну таємницю;

5) фіксація цифрових ідентифікаторів (контрольних сум) завантажених даних.

4. Під час здійснення пошуку відомостей у віртуальному середовищі (кіберпросторі) на основі відкритих джерел інформації можуть застосовуватися міжнародні стандарти документування відомостей з відкритих джерел, що не суперечить цьому Кодексу.»;

47. Частину 5 статті 245 викласти в такій редакції:

«5. Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису здійснюється у присутності слідчого, прокурора шляхом самостійного копіювання особою, яка є власником або володільцем відповідних приладів та засобів, або копіювання такою особою за участю спеціаліста відповідних записів на електронні носії інформації, які надаються слідчим, прокурором. Надання таких копій на електронних носіях інформації, особи, яка є власником або володільцем відповідних приладів та засобів, здійснюється за бажанням такої особи.»;

48. В частині 2 статті 246 цифри «263» виключити;

49. Частину 1 статті 263 доповнити абзацами наступного змісту:

«Нагляд та перехоплення даних змісту інформації є втручанням у приватне спілкування, що здійснюється без відома відповідних осіб та допускається виключно на підставі письмової та мотивованої ухвали слідчого судді.

Зняття інформації з електронних комунікаційних мереж та перехоплення даних змісту інформації можуть здійснюватися за наявності обґрунтованої підозри щодо особи, яка вчинила або бере участь у вчиненні тяжкого чи особливо тяжкого злочину, а також злочину у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку незалежно від їх тяжкості. Зазначені заходи можуть також застосовуватися щодо особи, яка за наявності обґрунтованої підозри передає або отримує від такої особи інформацію, що стосується зазначених злочинів, якщо злочинець використовує засоби зв'язку такої особи, а також якщо вона сприяє злочинцю.»;

50. Абзац 1 частини 4 статті 263 доповнити частиною наступного змісту:

«Нагляд та перехоплення даних змісту інформації здійснюють уповноважені підрозділи органів внутрішніх справ та органів безпеки, які зобов'язані невідкладно надіслати копію ухвали слідчого судді відповідному постачальнику електронних комунікаційних послуг.»;

51. Частину 4 статті 263 доповнити абзацом наступного змісту:

«Постачальники електронних комунікаційних послуг зобов'язані забезпечити технічну можливість проведення нагляду та перехоплення даних змісту інформації відповідно до вимог закону, забезпечити конфіденційність таких дій, вести облік випадків перехоплення інформації та надавати доступ до відповідних записів уповноваженим наглядовим органам у порядку, встановленому законом.»;

52. Доповнити новою статтею 264-1 «Доступ до інформації про спілкування та її аналіз (дані про рух інформації)» наступного змісту:

«Стаття 264-1. Доступ до інформації про спілкування та її аналіз (дані про рух інформації)

1. Отримання доступу до інформації про приватне спілкування особи та її аналіз є видом втручання у приватне спілкування, що здійснюється без відома осіб, яких це стосується. Інформація про приватне спілкування включає відомості, що можуть бути використані для встановлення особи учасників спілкування, тривалості, частоти та часу спілкування, а також місця перебування кінцевого обладнання електронних комунікацій.

2. Отримання доступу до інформації про приватне спілкування та її аналіз (даних про рух інформації) не передбачає доступу до змісту електронних комунікацій.

3. Отримання доступу до інформації про приватне спілкування та її аналіз (даних про рух інформації) здійснюється виключно на підставі ухвали слідчого судді, крім випадків, коли особа, щодо інформації про приватне спілкування якої йдеться, надала на це письмову згоду. У цьому випадку доступу до інформації про приватне спілкування та її аналіз (даних про рух інформації) здійснюється з відома особи і не є втручанням у приватне спілкування та здійснюється в порядку ст. 166-1 цього Кодексу.

4. Постачальники електронних комунікаційних послуг, їх керівники та уповноважені працівники зобов'язані забезпечити виконання технічних та інших вимог, необхідних для забезпечення доступу до інформації про приватне спілкування (даних про рух інформації) у режимі реального часу відповідно до вимог закону, забезпечити нерозголошення факту проведення таких дій та отриманих відомостей, а також вести облік усіх випадків надання доступу до такої інформації і надавати відповідні відомості уповноваженим органам у порядку, встановленому законом.»;

53. В частині 2 статті 265 слово «носієві» замінити на «електронному носієві інформації»;

54. В частинах 2 та 3 статті 266 слова «Носії інформації» замінити на «Електронні носії інформації»;

55. Частину 3 статті 290 доповнити абзацом наступного змісту:

«У разі відкриття доказів електронної форми забезпечується доступ до технічних атрибутів таких доказів, у тому числі до: цифрових ідентифікаторів

(контрольних сум) первинних електронних даних та їх копій; журналів ланцюга збереження; інформації про програмне й апаратне середовище, інструменти та методи, використані для одержання, збереження та дослідження таких доказів; службових і технічних метаданих; а також можливість використання програмних та технічних засобів для їх копіювання або передачі.»;

56. Частину 4 статті 290 доповнити абзацом наступного змісту:

«Надання доступу до доказів електронної форми включає право сторін кримінального провадження на отримання технічної інформації, необхідної для незалежної перевірки автентичності та цілісності таких доказів.»;

57. Частину 1 статті 567 доповнити словами «, у тому числі шляхом проведення процесуальних дій у режимі відеоконференції.»;

58. Частину 1 статті 567 викласти в такій редакції:

«1. За запитом компетентного органу іноземної держави допит особи може бути проведено за допомогою відео- або телефонної конференції. Такий допит проводиться у присутності слідчого судді за місцезнаходженням особи.»;

59. Частину 5 статті 567 викласти в такій редакції:

«5. Протокол допиту та носії відео- або аудіоінформації надсилаються до компетентного органу запитуючої сторони із забезпеченням ідентифікації даних та підтвердження їх цілісності.»;

60. Статтю 567 доповнити частиною 7 наступного змісту:

«7. Проведення допиту, впізнання, очної ставки чи інших процесуальних дій у режимі відеоконференції на підставі запиту про міжнародну правову допомогу здійснюється з урахуванням вимог статті 232 цього Кодексу.».

II. Прикінцеві та перехідні положення

1. Цей Закон набирає чинності з дня, наступного за його опублікуванням.

2. Зміни до статей 93-1, 100-1 набувають чинності з 01.07.2027.

3. Зміни до статті 94-1 набувають чинності з 01.07.2028.

4. Кабінету Міністрів України протягом трьох місяців з дня опублікування цього Закону розробити інструкцію щодо забезпечення взаємодії органів досудового розслідування та органів прокуратури з національним контактним пунктом 24/7, що забезпечує реалізацію процедур, визначених ст. 35 Конвенції про кіберзлочинність.

5. Кабінету Міністрів України протягом шести місяців з дня опублікування цього Закону розробити та затвердити нормативно-правові акти, що визначають:

перелік категорій даних, які підлягають зберіганню операторами та постачальниками електронних комунікаційних послуг у межах кримінального провадження;

порядок, строки, умови та вимоги до зберігання таких даних;

порядок доступу до цих даних органів досудового розслідування і прокуратури за рішенням слідчого судді;

заходи із забезпечення захисту права особи на приватність, недоторканність приватного життя та конфіденційність електронних комунікацій;

вимоги до фіксації, передачі, зберігання та захисту інформації, отриманої під час кримінального провадження із застосуванням електронних засобів телекомунікації.

привести власні нормативно-правові акти у відповідність із положеннями цього Закону та забезпечити узгодження нових актів із Законом України «Про електронні комунікації».

6. Офісу Генерального прокурора, Міністерству цифрової трансформації України та Міністерству юстиції України протягом одного року з дня набрання чинності цим Законом створити віртуальні архіви для зберігання доказів електронної форми, розробити та затвердити порядок зберігання резервних копій доказів електронної форми у таких віртуальних архівах. У разі необхідності, протягом трьох місяців з дня набрання чинності цим Законом спільно з Кабінетом Міністрів України розробити та подати до Верховної Ради України проєкт змін до законодавства у цій частині.

7. Офісу Генерального прокурора, Міністерству юстиції України, Національному агентству України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, Національному антикорупційному бюро України, Бюро економічної безпеки України, Державному бюро розслідувань, Службі безпеки України, Національній поліції України, Державній службі фінансового моніторингу України протягом одного року з дня набрання чинності цим Законом розробити та затвердити стандартні операційні процедури для роботи з доказами електронної форми під час кримінального провадження. У разі необхідності, протягом трьох місяців з дня набрання чинності цим Законом спільно з Кабінетом Міністрів України розробити та подати до Верховної Ради України проєкт змін до законодавства у цій частині.

ЗАКОН УКРАЇНИ**Про внесення змін та доповнень до деяких законодавчих актів
України щодо врегулювання роботи з доказами електронної форми**

Верховна Рада України п о с т а н о в л я є:

І. Внести до Цивільного процесуального кодексу України (Відомості Верховної Ради України (ВВР), 2004, № 40-41, 42, ст.492, із подальшими змінами) такі зміни:

1. Доповнити новою статтею 101-1 «Автентичність та цілісність доказів» наступного змісту:

«Стаття 101-1. Автентичність та цілісність доказів

1. Сторони та інші учасники цивільного процесу, а також суд зобов'язані забезпечити, щоб під час одержання, подання, зберігання та дослідження електронних доказів були вжиті заходи, спрямовані на недопущення їх зміни, пошкодження, знищення або спотворення.

2. У разі подання та дослідження електронної доказів забезпечується перевірка їх автентичності та цілісності шляхом застосування технічних і процесуальних засобів, зокрема фіксації метаданих, цифрових ідентифікаторів (контрольних сум), журналів дій доступу до даних, а також інших засобів верифікації та підтвердження автентичності й незмінності інформації.

3. Учасники процесу, які подають докази, зобов'язані забезпечити можливість подальшої перевірки їх походження, способу одержання, технічних параметрів та засобів забезпечення цілісності.

4. Відмова від застосування технічних способів забезпечення цілісності електронних доказів допускається лише у випадках, коли такі способи є об'єктивно неможливими, із документальним підтвердженням відповідних підстав та обставин.

5. Докази, щодо яких існують обґрунтовані сумніви в їх автентичності або цілісності, підлягають перевірці. У разі встановлення втручання, спотворення або порушення способу їх одержання та зберігання, що вплинуло на достовірність відомостей, такі докази можуть бути визнані недопустимими.».

II. Внести до Господарського процесуального кодексу України (Відомості Верховної Ради України (ВВР), 1992, № 6, ст.56, із подальшими змінами) такі зміни:

1. Доповнити новою статтею 97-1 «Автентичність та цілісність доказів» наступного змісту:

«Стаття 97-1. Автентичність та цілісність доказів

1. Сторони та інші учасники господарського процесу, а також суд зобов'язані забезпечити, щоб під час одержання, подання, зберігання та дослідження електронних доказів були вжиті заходи, спрямовані на недопущення їх зміни, пошкодження, знищення або спотворення.

2. У разі подання та дослідження електронної доказів забезпечується перевірка їх автентичності та цілісності шляхом застосування технічних і процесуальних засобів, зокрема фіксації метаданих, цифрових ідентифікаторів (контрольних сум), журналів дій доступу до даних, а також інших засобів верифікації та підтвердження автентичності й незмінності інформації.

3. Учасники процесу, які подають докази, зобов'язані забезпечити можливість подальшої перевірки їх походження, способу одержання, технічних параметрів та засобів забезпечення цілісності.

4. Відмова від застосування технічних способів забезпечення цілісності електронних доказів допускається лише у випадках, коли такі способи є об'єктивно неможливими, із документальним підтвердженням відповідних підстав та обставин.

5. Докази, щодо яких існують обґрунтовані сумніви в їх автентичності або цілісності, підлягають перевірці. У разі встановлення втручання, спотворення або порушення способу їх одержання та зберігання, що вплинуло на достовірність відомостей, такі докази можуть бути визнані недопустимими.».

III. Внести до Кодексу адміністративного судочинства України (Відомості Верховної Ради України (ВВР), 2005, № 35-36, № 37, ст.446, із подальшими змінами) такі зміни:

1. Доповнити новою статтею 100-1 «Автентичність та цілісність доказів» наступного змісту:

«Стаття 100-1. Автентичність та цілісність доказів

1. Сторони та інші учасники процесу, а також суд зобов'язані забезпечити, щоб під час одержання, подання, зберігання та дослідження електронних доказів були вжиті заходи, спрямовані на недопущення їх зміни, пошкодження, знищення або спотворення.

2. У разі подання та дослідження електронної доказів забезпечується перевірка їх автентичності та цілісності шляхом застосування технічних і процесуальних засобів, зокрема фіксації метаданих, цифрових ідентифікаторів

(контрольних сум), журналів дій доступу до даних, а також інших засобів верифікації та підтвердження автентичності й незмінності інформації.

3. Учасники процесу, які подають докази, зобов'язані забезпечити можливість подальшої перевірки їх походження, способу одержання, технічних параметрів та засобів забезпечення цілісності.

4. Відмова від застосування технічних способів забезпечення цілісності електронних доказів допускається лише у випадках, коли такі способи є об'єктивно неможливими, із документальним підтвердженням відповідних підстав та обставин.

5. Докази, щодо яких існують обґрунтовані сумніви в їх автентичності або цілісності, підлягають перевірці. У разі встановлення втручання, спотворення або порушення способу їх одержання та зберігання, що вплинуло на достовірність відомостей, такі докази можуть бути визнані недопустимими.».

IV. Зміни до інших Законів України.

1. Закон України «Про електронні комунікації» від 16 грудня 2020 року № 1089-IX (із наступними змінами) доповнити новими статтями 105-1 та 105-2 такого змісту:

«Стаття 105-1. Збереження електронних комунікаційних даних

1. Постачальники електронних комунікаційних послуг зобов'язані забезпечувати збереження електронних комунікаційних даних, визначених статтею 105-2 цього Закону, з метою:

1) здійснення досудового розслідування та судового розгляду у кримінальних провадженнях;

2) реалізації повноважень органів безпеки та правопорядку відповідно до спеціального законодавства;

3) надання доказів за запитами компетентних органів у порядку, визначеному законом.

2. Збереження даних здійснюється у тому вигляді, в якому вони формуються або обробляються у процесі надання електронних комунікаційних послуг. Постачальники не несуть обов'язок щодо накопичення або зберігання інформації, яка не створюється, не приймається або не опрацьовується ними у зв'язку з наданням послуг.

3. Строк збереження даних становить не більше дванадцяти місяців із дати їх отримання або створення, якщо інше не передбачено спеціальним законом.

4. Постачальники зобов'язані забезпечити, щоб збережені дані могли бути безперешкодно, своєчасно та в повному обсязі надані компетентним органам у порядку, визначеному законодавством.

5. Захист збережених даних має ґрунтуватися на таких принципах:

1) дані повинні зберігатися з рівнем безпеки, не нижчим від рівня захисту власних мереж та систем постачальника;

2) забороняється несанкціоноване копіювання, зміна, знищення або розголошення даних;

3) доступ до збережених даних здійснюється виключно уповноваженими особами відповідно до закону;

4) дані підлягають знищенню після закінчення строку їх зберігання або після зникнення потреби у їх використанні.

6. Постачальники забезпечують виконання вимог щодо зберігання і захисту даних шляхом упровадження організаційних і технічних заходів, фінансування яких здійснюється за рахунок власних ресурсів.

7. Кожен постачальник призначає посадову особу, відповідальну за дотримання вимог інформаційної безпеки та захисту персональних і комунікаційних даних.

8. Постачальники електронних комунікаційних послуг ведуть облік звернень компетентних органів про надання доступу до даних, із зазначенням правової підстави, дати запиту, виду даних та способу їх передачі. Зведена інформація про такі звернення надається на вимогу органів державного нагляду у сфері захисту інформації.

Стаття 105-2. Види даних, що підлягають збереженню

1. До електронних комунікаційних даних, що підлягають збереженню відповідно до статті 105-1 цього Закону, належать:

1) відомості, необхідні для ідентифікації джерела, з якого ініційовано електронне повідомлення;

2) відомості, що дозволяють встановити отримувача електронного повідомлення;

3) дані про дату, час початку, завершення та тривалість комунікації;

4) інформація про вид, технічний формат або протокол електронного повідомлення;

5) технічні ідентифікатори користувачів, обладнання, мережевих пристроїв і засобів доступу;

6) параметри, що ідентифікують обладнання користувачів мобільного зв'язку.

2. Дані, зазначені у частині першій цієї статті, можуть включати також інформацію про спроби з'єднання, що не були завершені, якщо їх фіксація передбачена технічною інфраструктурою постачальника.

3. Зміст повідомлень, переданих у процесі електронної комунікації, не підлягає збереженню або обробці, за винятком випадків, прямо передбачених законом.

4. Конкретний перелік категорій електронних комунікаційних даних, їх технічні формати, порядок фіксації, зберігання та знищення встановлюються нормативно-правовими актами центрального органу виконавчої влади у сфері електронних комунікацій та захисту інформації.

V. Прикінцеві положення

Кабінету Міністрів України у тримісячний строк з дня набрання чинності цим Законом:

розробити та затвердити вимоги до технічного та криптографічного захисту даних, що підлягають зберіганню;

розробити та затвердити порядок взаємодії між компетентними органами та постачальниками електронних комунікаційних послуг щодо запитів на доступ до даних;

привести свої нормативно-правові акти у відповідність із цим Законом.

ЗАТВЕРДЖУЮ

Проректор Національної академії
внутрішніх справ,
доктор юридичних наук, професор
полковник поліції

Олег ТАРАСЕНКО

2025 року

АКТ

10.07.2025

м. Київ

№ 124-НБ

Впровадження результатів дисертації
Каланчі Інги Георгіївни на тему «Докази
електронної форми у кримінальному процесі
України: теорія та практика» в наукову
діяльність НАВС

Уклала експертна комісія з виявлення, узагальнення та впровадження
позитивного досвіду роботи у складі:

- т.в.о. начальника відділу організації наукової діяльності, кандидата
юридичних наук старшого лейтенанта поліції Горбенко Дар'ї Андріївни;
- завідувача науково-дослідної лабораторії з проблем протидії злочинності
навчально-наукового інституту поліцейської діяльності, доктора юридичних наук,
професора майора поліції Вознюка Андрія Андрійовича;
- начальника відділу аспірантури (ад'юнктури) і докторантури, доктора
юридичних наук, професора підполковника поліції Тихонові Олени Вікторівни;
- завідувача кафедри кримінального процесу, доктора юридичних наук,
професора підполковника поліції Таран Олени Вікторівни;
- завідувача загальної бібліотеки Гайдар Людмили Георгіївни.

Комісія розглянула й узагальнила наукові праці здобувачки кафедри
кримінального процесу Національної академії внутрішніх Каланчі Інги Георгіївни
на тему «Докази електронної форми у кримінальному процесі України: теорія та
практика» поданої на здобуття наукового ступеня доктора юридичних наук зі
спеціальності 12.00.09 – кримінальний процес та криміналістика; судова
експертиза; оперативно-розшукова діяльність та на основі проведеного аналізу
зробила висновок, що надана наукові праці містить низку обґрунтованих
теоретичних положень і пропозицій спрямованих на теоретичне дослідження
доказів електронної форми у кримінальному процесі України.

Проаналізовано основні результати дослідження Каланчі І.Г., зокрема наукові
праці, в яких опубліковані теоретичні положення дисертації:

Каланча І.Г. Практика роботи з доказами, що мають електронну форму в
кримінальному процесі України : соціологічне дослідження. *Успіхи і досягнення у
науці*. №1(11). 2025. С. 76-93. DOI: [https://doi.org/10.52058/3041-1254-2025-1\(11\)-76-93](https://doi.org/10.52058/3041-1254-2025-1(11)-76-93)

Каланча І.Г. Електронний висновок експерта як доказ у кримінальному процесі України: практика, перспективи та ризики. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*, 2025. №2. С. 84-92. DOI <https://doi.org/10.32782/2311-8040/2025-2-12>

Каланча І.Г., Стемковський Д.Б. Використання доказів, що мають електронну форму в кримінальному процесі України: судова практика. Аналітично-порівняльне правознавство. 2025. №2. С. 1001-1008. DOI <https://doi.org/10.24144/2788-6018.2025.02.148> <https://app-journal.in.ua/wp-content/uploads/2025/04/150.pdf>

Kozii, V.; Kalancha, I.; Vlasova, H.; Orlean, A. Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies. *IDP. Internet, Law an Politics Journal*, 2025, no. 42. DOI: <http://dx.doi.org/10.7238/idp.v0i42.429924> URL: <https://raco.cat/index.php/IDP/article/view/429924/526486>

Каланча І.Г. Результати OSINT як джерело доказів у кримінальному процесі України. *Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій*: Матеріали Всеукр. наук.-практ. конф. (м. Чернівці, 20 грудня 2024 р.) / відп. ред. К.А. Возняковська. ТОМ 1, Чернівці, 2024. С. 43-49. URL: https://www.researchgate.net/publication/389647938_Kalanca_IG_Rezultati_OSINT_ak_dzerele_dokaziv_u_kriminalnomu_procesi_Ukraini_Innovacii_vikliki_ta_novi_horizon_ti_pravovogo_reguluvanna_u_svitli_suchasnih_socialno-ekonomichnih_ta_politichnih_transformaci

Каланча І. Термінологічне розмежування понять «електронний доказ», «цифровий доказ» і «доказ, що має електронну форму» в кримінальному процесі України. *Пріоритетні шляхи розвитку науки і освіти*: матеріали XV Міжнародної науково-практичної конференції м. Львів, 9-10 травня 2025 року. – Львів : Львівський науковий форум, 2025. С. 195-197. URL: <http://www.lviv-forum.inf.ua/save/2025/9-10.05/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA.pdf>

Каланча І.Г. Використання висновку експерта, що має електронну форму як доказу в кримінальному процесі України. Актуальні проблеми національного законодавства: збірник матеріалів Міжнародної науково-практичної конференції, м. Кропивницький, 17 квітня 2025 року. Частина 1. Кропивницький, 2025. С. 154-156. URL: https://www.researchgate.net/publication/392901845_Kalanca_IG_Vikoristanna_visnovku_eksperta_so_mae_elektronnu_formu_ak_dokazu_v_kriminalnomu_procesi_Ukraini_Aktualni_problemi_nacionalnogo_zakonodavstva_zbirnik_materialiv_Miznarodnoi_naukovo-prakticno

Patreliuk, D., Svoboda, I., Kalancha, I., Filashkin, V., Kachmar, B. Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations. *Pakistan Journal of Life and Social Sciences*, 2024, 22(2), pp. 4811–4820. DOI: <https://doi.org/10.57239/PJLSS-2024-22.2.00356> Scopus ID: 59332866200

Каланча І.Г. Алгоритм електронного кримінального провадження. *Law. State. Technology*, 2024. Вип. 4, С. 69–74. DOI: <https://doi.org/10.32782/LST/2024-4-13>

Каланча І.Г., Юрчишин Ю.В. Забезпечення безпеки прокурора під час роботи з електронним сегментом кримінального провадження в Україні. *Вчені записки*

Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки. Том 35 (74) № 6, 2024. С. 108-115. DOI: <https://doi.org/10.32782/TNU-2707-0581/2024.6/19>

Каланча І.Г., Орлеан А.М. Адаптація системи кримінальної юстиції до цифровізації світу : роль навчального компоненту. *Наукові перспективи*, №11 (53), 2024. С. 937-944. DOI: [https://doi.org/10.52058/2708-7530-2024-11\(53\)-937-944](https://doi.org/10.52058/2708-7530-2024-11(53)-937-944)

Каланча І.Г. Цифрова складова кримінального процесу України в науці та практиці: структурно-функціональний аналіз. *Сучасні виклики та актуальні проблеми судової реформи в Україні: Матеріали VIII Міжнар. наук.-практ. конф. (31 жовтня 2024р., Чернівці)/ редкол.: О.В. Щербанюк та ін. - Чернівці: 2024. С. 229-233.* URL:

https://www.researchgate.net/publication/390005117_Kalanca_IG_Cifrova_skladova_kriminalnogo_procesu_Ukraini_v_nauci_ta_praktici_strukturno-funkcionalnij_analiz_Sucasni_vikliki_ta_aktualni_problemi_sudovoi_reformi_v_Ukraini_Materiali_VIII_Miznar_nauk-p

Каланча І.Г. Способи ідентифікації комп'ютерних даних як доказу в кримінальному провадженні. *III Наукові читання пам'яті Ганса Гросса : збірник тез міжнародної науково-практичної конференції (м. Чернівці, 08 грудня 2023 р.). Чернівці: Чернівець. нац. У-нт. ім. Ю.Федьковича, 2023. С. 71-75. URL: <https://www.ndekc.cv.ua/wp-content/uploads/2024/03/III-Naukovi-chytannya-pam-yati-Gansa-Grossa.pdf>*

Каланча І.Г. Кіберпростір як територія проведення досудового розслідування. *Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини: зб. наук. праць за матер. Круглого столу, Київ, 7 грудня 2023 р. / редкол.: А.Ю. Нашинець-Наумова, Г.П. Власова, С.В. Бобровник, Т.О. Дідич, Н.А. Сергієнко, А.П. Чернега. - К. : Київ. стол. ун-т ім. Б. Грінченка, 2024. С. 115-119. URL: <https://kubg.edu.ua/struktura/pidrozdili/yurydychna-klinika-astreya/zakhody/8438-ikh-kruhlyi-stil-prava-liudyny-v-umovakh-voiennoho-stanu-v-ukraini.html>*

Каланча І.Г. Стратегії фіксації доказів, що мають електронну форму для застосування в кримінальному провадженні. *Сучасні виклики та актуальні проблеми судової реформи в Україні: Матеріали VII Міжнар. наук.-практ. конф. (27 жовтня 2023р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2023. С. 253-258. URL: https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk_conf_27..pdf*

Каланча І.Г. Окремі аспекти діяльності прокурора щодо гарантування цілісності доказів, що мають електронну форму під час досудового розслідування кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні: Матеріали VI Міжнар. наук.-практ. конф. (21 жовтня 2022р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2022. С. 327-332. URL: https://ccu.gov.ua/sites/default/files/suchasni_vyklyky_ta_aktualni_problemy_sudovoyi_reformy_v_ukrayini_2022.pdf*

Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*, №8, 2021. С. 336-339. DOI: <https://doi.org/10.32782/2524-0374/2021-8/77>

Гаркуша А.М., Каланча І.Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти.

Наукові читання пам'яті Ганса Гросса: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівський національний університет імені Юрія Федьковича. Чернівці : Технодрук, С. 72-75. URL:

http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/11383/Forensic_Epistemology_Czernowitz_2021_.pdf?sequence=1&isAllowed=y

Каланча І.Г. Підходи до класифікації електронних носіїв інформації та інформаційних систем для завдань кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні: Матеріали V Міжнар. наук.-практ. конф.* (29 жовтня 2021р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2021. С. 211-213. URL: <https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk-29.10.21.pdf>

Гаркуша А.М., Каланча І.Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи: матеріали круглого столу* (м. Львів, 11 червня 2021 р.). Львів: Львівський державний університет внутрішніх справ., 2021. С. 159-165. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/11_06_2021.pdf

Каланча І.Г. Інтероперабельність як обов'язкова властивість електронних інформаційних систем органів кримінальної юстиції. *Ročenka Ukrajinsko-Slovenská. Zborník vedeckých prác.* (Річник Українсько-Словацький. Збірник наукових праць) 2020. С. 64-70. URL: <https://www.eeda.sk/dok/publikacie/ostatne/2020-rocenka-ukrajinsko-slovenska.pdf>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законодавстві Молдови. *Jurnalul Juridic National: teorie si practica.* №1 (41). 2020. С. 132-137. URL: <http://www.jurnaluljuridic.in.ua/archive/2020/1/30.pdf>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Латвії. *Криміналістика і судова експертиза : міжвідомчий науково-методичний збірник.* Вип. 65, 2020. С. 90-100. DOI: <https://doi.org/10.33994/kndise.2020.65.09>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Вірменії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* №1. 2020. С. 205-210. DOI: <https://doi.org/10.31733/2078-3566-2020-1-205-210>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Туркменістану. *Актуальні проблеми вітчизняної юриспруденції.* № 1. 2020. С. 91-95. DOI: <https://doi.org/10.15421/392021> URL: http://apnl.dnu.in.ua/1_2020/23.pdf

Каланча І.Г. Поняття практики Європейського суду з прав людини як джерела кримінального процесуального права України. *Вісник кримінального судочинства.* № 2, 2020, С. 8-21. URL: https://vkslaw.knu.ua/images/verstka/Visnyk_Krim_Sud_3-4_20_231013_avt-8-21.pdf

Каланча І.Г. Тенденції та динаміка застосування практики Європейського суду з прав людини під час кримінального провадження: статистичне та соціологічне дослідження. *Теорія і практика правознавства,* Вип. 2(18), 2020. С. 14 (1-17). DOI: <https://doi.org/10.21564/2225-6555.2020.18.213676>

Каланча І.Г. Роль правових актів Європейського суду з прав людини в кримінальному процесі України. *Проблеми законності : зб. наук. праць.* № 150, 2020. С. 233-243. DOI: <https://doi.org/10.21564/2414-990x.150.209071>

Каланча І.Г. Шляхи формування сучасних практичних компетентностей у випускників правничих шкіл України. *Інноваційні рішення в сучасній науці, освіті та практиці*: Матеріали I Міжнародної науково-практичної інтернет-конференції (наукове видання), 17-18 листопада 2020 р.: у 2 ч. Київ: НТУ, 2020. Ч.2. С. 209-212. URL: <http://vstup.ntu.edu.ua/conf-innov-part-2.pdf>

Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. № 146, 2019. С. 179-191. DOI: <https://doi.org/10.21564/2414-990x.146.171218>

Каланча І.Г. Електронний сегмент в кримінальному процесі Грузії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №4. 2019. С. 161-166. DOI: <https://doi.org/10.31733/2078-3566-2019-4-161-166>

Каланча І.Г. Електронний сегмент кримінального процесу Естонії. *Порівняльно-аналітичне право*, №3, 2019. С. 212-216. URL: https://pap-journal.in.ua/wp-content/uploads/2021/07/3_2019.pdf

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Азербайджану. *Науковий вісник Ужгородського національного університету. Серія «Право»*. №59, 2019. С. 117-121. DOI: <https://doi.org/10.32782/2307-3322.59-2.26>

Каланча І.Г. Єдине електронне інформаційне поле органів кримінальної юстиції. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : мат. міжн. наук.-практ. конф. (м. Київ, 5.11.2019 р.). К., 2019. С. 209-213. URL:

https://www.researchgate.net/publication/393743748_Kalanca_IG_Edine_elektronne_in_formacijne_pole_organiv_kriminalnoi_usticii_Aktualni_pitanna_sudovoi_ekspertologii_kriminalistiki_ta_kriminalnogo_procesu_mat_mizn_nauk-prakt_konf_m_Kiiv_5112019_r_K_2019

На основі проведеного аналізу комісія зробила висновок про те, що вищезазначені матеріали Каланчі І.Г. можуть застосовуватися під час підготовки монографій, підручників, навчальних посібників, методичних рекомендацій, узагальнення аналітичних матеріалів, обґрунтування пропозицій до чинних проєктів нормативно-правових актів, підготовка яких потребує проведення відповідних наукових досліджень або містить наукову складову.

Члени комісії:

 Дар'я ГОРБЕНКО

 Андрій ВОЗНІЮК

 Олена ТИХОНОВА

 Олена ТАРАН

 Людмила ГАЙДАР

ЗАТВЕРДЖУЮ

Заступник декана факультету
права та міжнародних відносин
Київського столичного університету
імені Бориса Грінченка
доктор юридичних наук, професор



Анфіса НАШИНЕЦЬ-НАУМОВА

Нашинець-Наумова 2025 року

АКТ

«__» _____ 2025 року

м. Київ

про впровадження результатів
дисертаційного дослідження Каланчі Інги
Георгіївни на тему: «Докази електронної
форми в кримінальному процесі України:
теорія і практика» у наукову діяльність
Київського столичного університету імені
Бориса Грінченка

Комісія у складі:

завідувача кафедри публічного права факультету права та міжнародних
відносин Київського столичного університету імені Бориса Грінченка, доктора
юридичних наук, професора, заслуженого діяча науки і техніки України
Цимбал Ганни Петрівни,

професора кафедри публічного права факультету права та міжнародних
відносин Київського столичного університету імені Бориса Грінченка, доктора
юридичних наук, доцента Завидника Володимира Івановича,

доцента кафедри публічного права факультету права та міжнародних
відносин Київського столичного університету імені Бориса Грінченка, доктора
філософії в галузі права Лісіцького Андрія Валерійовича,

розглянула й узагальнила результати дисертаційного дослідження
здобувачки кафедри кримінального процесу Національної академії внутрішніх
справ Каланчі Інги Георгіївни на тему: «Докази електронної форми у
кримінальному процесі України: теорія та практика», поданого на здобуття
наукового ступеня доктора юридичних наук зі спеціальності 12.00.09 -

кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність.

На основі проведеного аналізу комісія встановила, що надані наукові праці Каланчі І.Г. містять комплекс обґрунтованих теоретичних положень, висновків і пропозицій, спрямованих на розвиток теорії доказування у кримінальному процесі України та вдосконалення наукових засад доказів електронної форми.

Проаналізовано основні результати дослідження, зокрема наукові праці Каланчі І.Г., у яких опубліковано положення дисертаційного дослідження:

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Азербайджану. *Науковий вісник Ужгородського національного університету. Серія «Право»*. №59. 2019. С. 117-121. DOI: <https://doi.org/10.32782/2307-3322.59-2.26>

Каланча І.Г. Електронний сегмент кримінального процесу Естонії. *Порівняльно-аналітичне право*, №3, 2019. С. 212-216. URL: https://pap-journal.in.ua/wp-content/uploads/2021/07/3_2019.pdf

Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. № 146, 2019. С. 179-191. DOI: <https://doi.org/10.21564/2414-990x.146.171218>

Каланча І.Г. Електронний сегмент в кримінальному процесі Грузії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №4. 2019. С. 161-166. DOI: <https://doi.org/10.31733/2078-3566-2019-4-161-166>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законодавстві Молдови. *Jurnalul Juridic National: teorie si practica*. №1 (41). 2020. С. 132-137. URL: <http://www.jurnaluljuridic.in.ua/archive/2020/1/30.pdf>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Туркменістану. *Актуальні проблеми вітчизняної юриспруденції*. № 1. 2020. С. 91-95. DOI: <https://doi.org/10.15421/392021> URL: http://apnl.dnu.in.ua/1_2020/23.pdf

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Вірменії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №1. 2020. С. 205-210. DOI: <https://doi.org/10.31733/2078-3566-2020-1-205-210>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Латвії. *Криміналістика і судова експертиза : міжвідомчий науково-методичний збірник*. Вип. 65, 2020. С. 90-100. DOI: <https://doi.org/10.33994/kndise.2020.65.09>

Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти.

Юридичний науковий електронний журнал, №8, 2021. С. 336-339. DOI: <https://doi.org/10.32782/2524-0374/2021-8/77>

Patreluk, D., Svoboda, I., Kalancha, I., Filashkin, V., Kachmar, B. Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations. *Pakistan Journal of Life and Social Sciences*, 2024, 22(2), pp. 4811–4820. DOI: <https://doi.org/10.57239/PJLSS-2024-22.2.00356>

Каланча І.Г., Орлеан А.М. Адаптація системи кримінальної юстиції до цифровізації світу : роль навчального компоненту. *Наукові перспективи*, №11 (53), 2024. С. 937-944. DOI: [https://doi.org/10.52058/2708-7530-2024-11\(53\)-937-944](https://doi.org/10.52058/2708-7530-2024-11(53)-937-944)

Каланча І.Г., Юрчишин Ю.В. Забезпечення безпеки прокурора під час роботи з електронним сегментом кримінального провадження в Україні. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки*. Том 35 (74) № 6, 2024. С. 108-115. DOI: <https://doi.org/10.32782/TNU-2707-0581/2024.6/19>

Каланча І.Г. Алгоритм електронного кримінального провадження. *Law. State. Technology*, 2024. Вип. 4, С. 69–74. DOI: <https://doi.org/10.32782/LST/2024-4-13>

Каланча І.Г. Практика роботи з доказами, що мають електронну форму в кримінальному процесі України : соціологічне дослідження. *Успіхи і досягнення у науці*. №1(11). 2025. С. 76-93. DOI: [https://doi.org/10.52058/3041-1254-2025-1\(11\)-76-93](https://doi.org/10.52058/3041-1254-2025-1(11)-76-93)

Каланча І.Г., Стемковський Д.Б. Використання доказів, що мають електронну форму в кримінальному процесі України: судова практика. Аналітично-порівняльне правознавство. 2025. №2. С. 1001-1008. DOI: <https://doi.org/10.24144/2788-6018.2025.02.148> <https://app-journal.in.ua/wp-content/uploads/2025/04/150.pdf>

Каланча І.Г. Електронний висновок експерта як доказ у кримінальному процесі України: практика, перспективи та ризики. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. №2. С. 84-92. DOI: <https://doi.org/10.32782/2311-8040/2025-2-12> URL: <http://journals.lvduvys.lviv.ua/index.php/law/article/view/981/953>

Каланча І.Г. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світлі концепції chain of custody. *Věda a perspektivy*. № 8(51) (2025). С. 206-230. URL: https://www.researchgate.net/publication/394998880_Kalanca_IG_Dokazi_so_maut_elektronnu_formu_v_kriminalnomu_procesi_Ukraini_identifikacia_ta_cilisni_st_u_svitli_koncepcii_chain_of_custody_Veda_a_perspektivy_No_851_2025_C_206-230

Kozii, V.; Kalancha, I.; Vlasova, H.; Orlean, A. Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine

using cryptocurrencies. *IDP. Internet, Law and Politics Journal*, 2025, no. 42, pp. 1-13. DOI: <http://dx.doi.org/10.7238/idp.v0i42.429924> URL: <https://raco.cat/index.php/IDP/article/view/429924/526486>

Каланча І.Г. Процесуальна природа доказів, що мають електронну форму в кримінальному процесі України: документ та речовий доказ. *Міжнародний науковий журнал "Інтернаука". Серія: "Юридичні науки"*. № 7. 2025. С. 85-92. DOI <https://doi.org/10.25313/2520-2308-2025-7-11208> URL: <https://www.inter-nauka.com/uploads/public/17557614844770.pdf>

Каланча І.Г. Організаційні аспекти роботи з доказами, що мають електронну форму в кримінальному процесі України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. Вип. 90, Ч. 4. 2025. С. 258-266. DOI <https://doi.org/10.24144/2307-3322.2025.90.4.36>

Каланча І.Г. Єдине електронне інформаційне поле органів кримінальної юстиції. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : мат. міжн. наук.-практ. конф. (м. Київ, 5.11.2019 р.). К., 2019. С. 209-213. URL: https://www.researchgate.net/publication/393743748_Kalanca_IG_Edine_elektronne_informacijne_pole_organiv_kriminalnoi_usticii_Aktualni_pitannya_sudovoi_ekspernologii_kriminalistiki_ta_kriminalnogo_procesu_mat_mizn_nauk-prakt_conf_m_Kiiv_5112019_r_K_2019

Каланча І.Г. Шляхи формування сучасних практичних компетентностей у випускників правничих шкіл України. *Інноваційні рішення в сучасній науці, освіті та практиці*: Матеріали I Міжнародної науково-практичної інтернет-конференції (наукове видання), 17-18 листопада 2020 р.: у 2 ч. Київ: НТУ, 2020. Ч.2. С. 209-212. URL: <http://vstup.ntu.edu.ua/conf-innov-part-2.pdf>

Гаркуша А.М., Каланча І.Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи*: матеріали круглого столу (м. Львів, 11 червня 2021 р.). Львів: Львівський державний університет внутрішніх справ., 2021. С. 159-165. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/11_06_2021.pdf

Каланча І.Г. Підходи до класифікації електронних носіїв інформації та інформаційних систем для завдань кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали V Міжнар. наук.-практ. конф. (29 жовтня 2021р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2021. С. 211-213. URL: <https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk-29.10.21.pdf>

Гаркуша А.М., Каланча І.Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. *Наукові читання пам'яті Ганса Гросса*: збірник тез міжнародної науково-

практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівецький національний університет імені Юрія Федьковича. Чернівці : Технодрук, С. 72-75.

URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/11383/Forensic_Epi stemology_Czernowitz_2021_.pdf?sequence=1&isAllowed=y

Каланча І.Г. Окремі аспекти діяльності прокурора щодо гарантування цілісності доказів, що мають електронну форму під час досудового розслідування кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VI Міжнар. наук.-практ. конф. (21 жовтня 2022р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2022. С. 327-332.

URL: https://ccu.gov.ua/sites/default/files/suchasni_vyklyky_ta_aktualni_problemy_sudovoi_reformy_v_ukrayini_2022.pdf

Каланча І.Г. Способи ідентифікації комп'ютерних даних як доказу в кримінальному провадженні. *III Наукові читання пам'яті Ганса Гросса* : збірник тез міжнародної науково-практичної конференції (м. Чернівці, 08 грудня 2023 р.). Чернівці: Чернівец. нац. У-нт. ім. Ю.Федьковича, 2023. С. 71-75. URL: <https://www.ndekc.cv.ua/wp-content/uploads/2024/03/III-Naukovi-chytannya-pam-yati-Gansa-Grossa.pdf>

Каланча І.Г. Стратегії фіксації доказів, що мають електронну форму для застосування в кримінальному провадженні. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VII Міжнар. наук.-практ. конф. (27 жовтня 2023р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2023. С. 253-258.

URL: https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk_conf_27..pdf

Каланча І.Г. Кіберпростір як територія проведення досудового розслідування. *Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини*: зб. наук. праць за матер. Круглого столу, Київ, 7 грудня 2023 р. / редкол.: А.Ю. Нашинець-Наумова, Г.П. Власова, С.В. Бобровник, Т.О. Дідич, Н.А. Сергієнко, А.П. Чернега. – К. : Київ. стол. ун-т ім. Б. Грінченка, 2024. С. 115-119. URL: <https://kuhg.edu.ua/struktura/pidrozdi/yurydychna-klinika-astreya/zakhody/8438-ikh-kruhlyi-stil-prava-liudyny-v-umovakh-voiennoho-stanu-v-ukraini.html>

Каланча І.Г. Цифрова складова кримінального процесу України в науці та практиці: структурно-функціональний аналіз. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VIII Міжнар. наук.-практ. конф. (31 жовтня 2024р., Чернівці)/ редкол.: О.В. Щербанюк та ін. - Чернівці: 2024. С. 229-233.

URL: https://www.researchgate.net/publication/390005117_Kalanca_IG_Cifrova_sklado_va_kriminalnogo_procesu_Ukraini_v_nauci_ta_praktici_strukturno-funkcionalnij_analiz_Sucasni_viklyki_ta_aktualni_problemi_sudovoi_reformi_v_Ukraini_Materiali_VIII_Miznar_nauk-p

Каланча І.Г. Матеріальна форма існування як властивість доказу в кримінальному процесі України: практика правозастосування. *Права людини в умовах воєнного стану в Україні: X круглий стіл до Всеукраїнського тижня права (10 грудня 2024 року). Права людини в умовах воєнного стану в Україні: до тижня права і Загальної декларації прав людини* : зб. наук. праць за матер. круглого столу, Київ, 10 грудня 2024 р. / редкол.: А.Ю. Нашинець-Наумова, Г.П. Цимбал, С.В. Бобровник, Т.О. Дідич, О.І. Чаплюк, А.П. Чернега. — Київ : Київ. столич. ун-т ім. Б. Грінченка, 2025. С. 63-67. URL: https://www.researchgate.net/publication/396154856_Kalanca_IG_Materialna_forma_isnuvanna_ak_vlastivist_dokazu_v_kriminalnomu_procesi_Ukraini_praktika_pravozastosuvannya_Prava_ludini_v_umovah_voennogo_stanu_v_Ukraini_X_kruglij_stil_do_Vseukrainskogo_tiz

Каланча І. Термінологічне розмежування понять «електронний доказ», «цифровий доказ» і «доказ, що має електронну форму» в кримінальному процесі України. *Пріоритетні шляхи розвитку науки і освіти: матеріали XV Міжнародної науково-практичної конференції* м. Львів, 9-10 травня 2025 року. — Львів : Львівський науковий форум, 2025. С. 195-197. URL: <http://www.lviv-forum.inf.ua/save/2025/9-10.05/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA.pdf>

Власова Г.П., Каланча І.Г. Захисник як суб'єкт роботи з електронними доказами в кримінальному провадженні. *Актуальні питання реформування правової системи* : зб. матеріалів XXII Міжнар. наук.-практ. конф., Луцьк, 13-15 червня 2025 р. / Уклад. Джурак Л. М. — Луцьк : Вежа-Друк, 2025. С. 113-115. URL: https://www.law.vnu.edu.ua/files/ugd/65dd18_5ab2de833d004115b0483aa2420d7cc0.pdf

Каланча І.Г. Результати OSINT як джерело доказів у кримінальному процесі України. *Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій: Матеріали Всеукр. наук.-практ. конф. (м. Чернівці, 20 грудня 2024 р.)* / відп. ред. К.А. Возняковська. ТОМ 1, Чернівці, 2024. С. 43-49. URL: https://www.researchgate.net/publication/389647938_Kalanca_IG_Rezultati_OSINT_ak_dzerelo_dokaziv_u_kriminalnomu_procesi_Ukraini_Innovacii_vikliki_ta_novi_gorizonti_pravovogo_reguluvannya_u_svitli_sucasnih_socialno-ekonomichnih_ta_politicnih_transformaci

Каланча І.Г. Використання висновку експерта, що має електронну форму як доказу в кримінальному процесі України. *Актуальні проблеми національного законодавства: збірник матеріалів Міжнародної науково-практичної конференції*, м. Кропивницький, 17 квітня 2025 року. Частина 1, Кропивницький, 2025. С. 154-156. URL: https://www.researchgate.net/publication/392901845_Kalanca_IG_Vikoristannya_v_isnovku_eksperta_so_mae_elektronnu_formu_ak_dokazu_v_kriminalnomu_proces

i Ukraini Aktualni problemi nacionalnogo zakonodavstva zbirnik materialiv Miznarodnoi naukovoprakticno

На підставі проведеного аналізу комісія дійшла висновку, що наукові публікації Каланчі І.Г. є науково обґрунтованими, теоретично значущими та можуть бути використані у науковій діяльності, а саме: при підготовці монографій, підручників, навчальних посібників і методичних рекомендацій; у процесі розроблення аналітичних матеріалів, експертних висновків і наукових узагальнень; під час обґрунтування пропозицій до чинних або проєктів нормативно-правових актів, розроблення яких потребує проведення наукових досліджень або містить наукову складову; при підготовці дисертаційних досліджень здобувачів у галузі кримінального процесу та суміжних правових дисциплін.

Члени комісії:

Завідувач кафедри публічного права
факультету права та міжнародних відносин
Київського столичного університету
імені Бориса Грінченка,
доктор юридичних наук, професор,
заслужений діяч науки і техніки України



Ганна ЦИМБАЛ

Професор кафедри публічного права
факультету права та міжнародних відносин
Київського столичного університету
імені Бориса Грінченка,
доктор юридичних наук, доцент



Володимир ЗАВИДНЯК

Доцент кафедри публічного права
факультету права та міжнародних відносин
Київського столичного університету
імені Бориса Грінченка,
доктор філософії в галузі права



Андрій ЛІСЦЬКИЙ

ЗАТВЕРДЖУЮ

Проректор з наукової роботи ПВНЗ
«Європейський університет»,
доктор економічних наук, професор


 Кузь Ю.Ф.

« » _____ 2025 року

АКТ впровадження результатів дисертаційного дослідження Каланчі Інги Георгіївни на тему: «Докази електронної форми в кримінальному процесі України: теорія і практика» у наукову діяльність.

«20» жовтня 2025 року

м. Київ

Комісія у складі:

завідувача кафедри права ПВНЗ «Європейський університет»
доктора юридичних наук, професора, заслуженого юриста України
Цимбала Петра Васильовича,

професора кафедри права ПВНЗ «Європейський університет»
кандидата юридичних наук, доцента Тимошенко Ольги Анатоліївни,

директора Центру забезпечення якості освіти ПВНЗ «Європейський
університет» кандидата юридичних наук, доцента Кузьменко Олени
Валеріївни,

розглянула й узагальнила результати дисертаційного дослідження
здобувачки кафедри кримінального процесу Національної академії внутрішніх
справ Каланчі Інги Георгіївни на тему: «Докази електронної форми у
кримінальному процесі України: теорія та практика», поданого на здобуття
наукового ступеня доктора юридичних наук зі спеціальності 12.00.09 -
кримінальний процес та криміналістика; судова експертиза; оперативно-
розшукова діяльність.

На основі проведеного аналізу комісія встановила, що надані наукові
праці Каланчі І.Г. містять комплекс обґрунтованих теоретичних положень,
висновків і пропозицій, спрямованих на розвиток теорії доказування у
кримінальному процесі України та вдосконалення наукових засад доказів
електронної форми.

Проаналізовано основні результати дослідження, зокрема наукові праці Каланчі І.Г., у яких опубліковано положення дисертаційного дослідження:

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Азербайджану. *Науковий вісник Ужгородського національного університету. Серія «Право»*. №59. 2019. С. 117-121. DOI: <https://doi.org/10.32782/2307-3322.59-2.26>

Каланча І.Г. Електронний сегмент кримінального процесу Естонії. *Порівняльно-аналітичне право*, №3, 2019. С. 212-216. URL: https://pap-journal.in.ua/wp-content/uploads/2021/07/3_2019.pdf

Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. № 146, 2019. С. 179-191. DOI: <https://doi.org/10.21564/2414-990x.146.171218>

Каланча І.Г. Електронний сегмент в кримінальному процесі Грузії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №4, 2019. С. 161-166. DOI: <https://doi.org/10.31733/2078-3566-2019-4-161-166>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законодавстві Молдови. *Jurnalul Juridic National: teorie si practica*. №1 (41). 2020. С. 132-137. URL: <http://www.jurnaluljuridic.in.ua/archive/2020/1/30.pdf>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Туркменістану. *Актуальні проблеми вітчизняної юриспруденції*. № 1, 2020. С. 91-95. DOI: <https://doi.org/10.15421/392021> URL: http://apnl.dnu.in.ua/1_2020/23.pdf

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Вірменії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №1, 2020. С. 205-210. DOI: <https://doi.org/10.31733/2078-3566-2020-1-205-210>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Латвії. *Криміналістика і судова експертиза : міжвідомчий науково-методичний збірник*. Вип. 65, 2020. С. 90-100. DOI: <https://doi.org/10.33994/kndise.2020.65.09>

Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*, №8, 2021. С. 336-339. DOI: <https://doi.org/10.32782/2524-0374/2021-8/77>

Patreliuk, D., Svoboda, I., Kalancha, I., Filashkin, V., Kachmar, B. Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations. *Pakistan Journal of Life and Social Sciences*, 2024, 22(2), pp. 4811–4820. DOI: <https://doi.org/10.57239/PJLSS-2024-22.2.00356>

(53), 2024. С. 937-944. DOI: [https://doi.org/10.52058/2708-7530-2024-11\(53\)-937-944](https://doi.org/10.52058/2708-7530-2024-11(53)-937-944)

Каланча І.Г., Юрчишин Ю.В. Забезпечення безпеки прокурора під час роботи з електронним сегментом кримінального провадження в Україні. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки*. Том 35 (74) № 6, 2024. С. 108-115. DOI: <https://doi.org/10.32782/TNU-2707-0581/2024.6/19>

Каланча І.Г. Алгоритм електронного кримінального провадження. *Law. State. Technology*, 2024. Вип. 4, С. 69-74. DOI: <https://doi.org/10.32782/LST/2024-4-13>

Каланча І.Г. Практика роботи з доказами, що мають електронну форму в кримінальному процесі України : соціологічне дослідження. *Успіхи і досягнення у науці*. №1(11). 2025. С. 76-93. DOI: [https://doi.org/10.52058/3041-1254-2025-1\(11\)-76-93](https://doi.org/10.52058/3041-1254-2025-1(11)-76-93)

Каланча І.Г., Стемковський Д.Б. Використання доказів, що мають електронну форму в кримінальному процесі України: судова практика. *Аналітично-порівняльне правознавство*. 2025. №2. С. 1001-1008. DOI: <https://doi.org/10.24144/2788-6018.2025.02.148> <https://app-journal.in.ua/wp-content/uploads/2025/04/150.pdf>

Каланча І.Г. Електронний висновок експерта як доказ у кримінальному процесі України: практика, перспективи та ризики. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. №2. С. 84-92. DOI: <https://doi.org/10.32782/2311-8040/2025-2-12> URL: <http://journals.lvduvs.lviv.ua/index.php/law/article/view/981/953>

Каланча І.Г. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світлі концепції chain of custody. *Věda a perspektivy*. № 8(51) (2025). С. 206-230. URL: https://www.researchgate.net/publication/394998880_Kalanca_I_G_Dokazi_so_maut_elektronnu_formu_v_kriminalnomu_procesi_Ukraini_identifikacia_ta_cilisni_st_u_svitli_koncepcii_chain_of_custody_Veda_a_perspektivy_No_851_2025_C_206-230

Kozii, V.; Kalancha, I.; Vlasova, H.; Orlean, A. Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies. *IDP. Internet, Law an Politics Journal*, 2025, no. 42. pp. 1-13. DOI: <http://dx.doi.org/10.7238/idp.v0i42.429924> URL: <https://raco.cat/index.php/IDP/article/view/429924/526486>

Каланча І.Г. Процесуальна природа доказів, що мають електронну форму в кримінальному процесі України: документ та речовий доказ. *Міжнародний науковий журнал "Інтернаука". Серія: "Юридичні науки"*. № 7. 2025. С. 85-92. DOI <https://doi.org/10.25313/2520-2308-2025-7-11208> URL: <https://www.inter-nauka.com/uploads/public/17557614844770.pdf>

Каланча І.Г. Організаційні аспекти роботи з доказами, що мають електронну форму в кримінальному процесі України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. Вип. 90, Ч. 4. 2025. С. 258-266. DOI <https://doi.org/10.24144/2307-3322.2025.90.4.36>

Каланча І.Г. Єдине електронне інформаційне поле органів кримінальної юстиції. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : мат. міжн. наук.-практ. конф. (м. Київ, 5.11.2019 р.). К., 2019. С. 209-213. URL: https://www.researchgate.net/publication/393743748_Kalanca_IG_Edine_elektronne_informacijne_pole_organiv_kriminalnoi_usticii_Aktualni_pitanna_sudovoi_ekspernologii_kriminalistiki_ta_kriminalnogo_procesu_mat_mizn_nauk-prakt_konf_m_Kiiv_5112019_r_K_2019

Каланча І.Г. Шляхи формування сучасних практичних компетентностей у випускників правничих шкіл України. *Інноваційні рішення в сучасній науці, освіті та практиці*: Матеріали I Міжнародної науково-практичної інтернет-конференції (наукове видання), 17-18 листопада 2020 р.: у 2 ч. Київ: НТУ, 2020. Ч.2. С. 209-212. URL: <http://vstup.ntu.edu.ua/conf-innov-part-2.pdf>

Гаркуша А.М., Каланча І.Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи*: матеріали круглого столу (м. Львів, 11 червня 2021 р.). Львів: Львівський державний університет внутрішніх справ., 2021. С. 159-165. URL: https://www.lvduvs.edu.ua/documents/pdf/biblioteka/nauk_konf/11_06_2021.pdf

Каланча І.Г. Підходи до класифікації електронних носіїв інформації та інформаційних систем для завдань кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали V Міжнар. наук.-практ. конф. (29 жовтня 2021р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2021. С. 211-213. URL: <https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk-29.10.21.pdf>

Гаркуша А.М., Каланча І.Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. *Наукові читання пам'яті Ганса Гросса*: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівецький національний університет імені Юрія Федьковича. Чернівці : Технодрук, С. 72-75. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/11383/Forensic_Epi_stemology_Czernowitz_2021_.pdf?sequence=1&isAllowed=y

Каланча І.Г. Окремі аспекти діяльності прокурора щодо гарантування цілісності доказів, що мають електронну форму під час досудового розслідування кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VI Міжнар. наук.-практ. конф.

(21 жовтня 2022р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2022. С. 327-332. URL: https://ccu.gov.ua/sites/default/files/suchasni_vyklyky_ta_aktualni_problemy_sudovoi_reformy_v_ukrayini_2022.pdf

Каланча І.Г. Способи ідентифікації комп'ютерних даних як доказу в кримінальному провадженні. *III Наукові читання пам'яті Ганса Гросса* : збірник тез міжнародної науково-практичної конференції (м. Чернівці, 08 грудня 2023 р.). Чернівці: Чернівець. нац. У-нт. ім. Ю.Федьковича, 2023. С. 71-75. URL: <https://www.ndekc.cv.ua/wp-content/uploads/2024/03/III-Naukovi-chytannya-pam-yati-Gansa-Grossa.pdf>

Каланча І.Г. Стратегії фіксації доказів, що мають електронну форму для застосування в кримінальному провадженні. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VII Міжнар. наук.-практ. конф. (27 жовтня 2023р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2023. С. 253-258. URL: https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk_conf_27..pdf

Каланча І.Г. Кіберпростір як територія проведення досудового розслідування. *Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини*: зб. наук. праць за матер. Круглого столу, Київ, 7 грудня 2023 р. / редкол.: А.Ю. Нашинець-Наумова, Г.П. Власова, С.В. Бобровник, Т.О. Дідич, Н.А. Сергієнко, А.П. Чернега. – К. : Київ. стол. ун-т ім. Б. Грінченка, 2024. С. 115-119. URL: <https://kubg.edu.ua/struktura/pidrozdili/yurydychna-klinika-astreya/zakhody/8438-ikh-kruhlyi-stil-prava-liudyny-v-umovakh-voiennoho-stanu-v-ukraini.html>

Каланча І.Г. Цифрова складова кримінального процесу України в науці та практиці: структурно-функціональний аналіз. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VIII Міжнар. наук.-практ. конф. (31 жовтня 2024р., Чернівці)/ редкол.: О.В. Щербанюк та ін. - Чернівці: 2024. С. 229-233. URL: https://www.researchgate.net/publication/390005117_Kalanca_IG_Cifrova_skladova_kriminalnogo_procesu_Ukraini_v_nauci_ta_praktici_strukturno-funkcionalnij_analiz_Sucasni_vikliki_ta_aktualni_problemi_sudovoi_reformi_v_Ukraini_Materiali_VIII_Miznar_nauk-p

Каланча І.Г. Матеріальна форма існування як властивість доказу в кримінальному процесі України: практика правозастосування. *Права людини в умовах воєнного стану в Україні: X круглий стіл до Всеукраїнського тижня права (10 грудня 2024 року). Права людини в умовах воєнного стану в Україні: до тижня права і Загальної декларації прав людини* : зб. наук. праць за матер. круглого столу, Київ, 10 грудня 2024 р. / редкол.: А.Ю. Нашинець-Наумова, Г.П. Цимбал, С.В. Бобровник, Т.О. Дідич, О.І. Чаплук, А.П. Чернега. — Київ : Київ. столич. ун-т ім. Б. Грінченка, 2025. С. 63-67. URL: https://www.researchgate.net/publication/396154856_Kalanca_IG_Materialna_forma_isnuvannya_yak_vlastivist_dokazu_v_kriminalnomu_procesi_Ukraini_praктика_pravozastosuвання

ma isnuvanna ak vlastivist dokazu v kriminalnomu procesi Ukraini praktika pravozastosuvanna Prava ludini v umovah voennogo stanu v Ukraini X krugl ij stil do Vseukrainskogo tiz

Каланча І. Термінологічне розмежування понять «електронний доказ», «цифровий доказ» і «доказ, що має електронну форму» в кримінальному процесі України. *Пріоритетні шляхи розвитку науки і освіти: матеріали XV Міжнародної науково-практичної конференції* м. Львів, 9-10 травня 2025 року. – Львів : Львівський науковий форум, 2025. С. 195-197. URL: <http://www.lviv-forum.inf.ua/save/2025/9-10.05/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA.pdf>

Власова Г.П., Каланча І.Г. Захисник як суб'єкт роботи з електронними доказами в кримінальному провадженні. *Актуальні питання реформування правової системи : зб. матеріалів XXII Міжнар. наук.-практ. конф., Луцьк, 13-15 червня 2025 р. / Уклад. Джурак Л. М. – Луцьк : Вежа-Друк, 2025. С. 113-115.* URL: https://www.law.vnu.edu.ua/_files/ugd/65dd18_5ab2de833d004115b0483aa2420d7cc0.pdf

Каланча І.Г. Результати OSINT як джерело доказів у кримінальному процесі України. *Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій: Матеріали Всеукр. наук.-практ. конф. (м. Чернівці, 20 грудня 2024 р.) / відп. ред. К.А. Возняковська. ТОМ 1, Чернівці, 2024. С. 43-49.* URL: https://www.researchgate.net/publication/389647938_Kalanca_IG_Rezultati_OSINT_ak_dzerelo_dokaziv_u_kriminalnomu_procesi_Ukraini_Innovacii_vikliki_ta_novi_gorizonti_pravovogo_reguluvanna_u_svitli_sucasnih_socialno-ekonomichnih_ta_politicnih_transformaci

Каланча І.Г. Використання висновку експерта, що має електронну форму як доказу в кримінальному процесі України. *Актуальні проблеми національного законодавства: збірник матеріалів Міжнародної науково-практичної конференції, м. Кропивницький, 17 квітня 2025 року. Частина 1. Кропивницький, 2025. С. 154-156.* URL: https://www.researchgate.net/publication/392901845_Kalanca_IG_Vikoristanna_v_isnovku_eksperta_so_mae_elektronnu_formu_ak_dokazu_v_kriminalnomu_procesi_Ukraini_Aktualni_problemi_nacionalnogo_zakonodavstva_zbirnik_materialiv_Miznarodnoi_naukovo-prakticno

На підставі проведеного аналізу комісія дійшла висновку, що наукові публікації Каланчі І.Г. є науково обґрунтованими, теоретично значущими та можуть бути використані у науковій діяльності, а саме: при підготовці монографій, підручників, навчальних посібників і методичних рекомендацій; у процесі розроблення аналітичних матеріалів, експертних висновків і наукових узагальнень; під час обґрунтування пропозицій до чинних або проектів нормативно-правових актів, розроблення яких потребує проведення

наукових досліджень або містить наукову складову; при підготовці дисертаційних досліджень здобувачів у галузі кримінального процесу та суміжних правових дисциплін.

Члени комісії:

**Завідувач кафедри права
ПВНЗ «Європейський університет»
доктор юридичних наук, професор,
заслужений юрист України**



Петро ЦИМБАЛ

**Професор кафедри права
ПВНЗ «Європейський університет»
кандидат юридичних наук,
доцент**



Ольга ТИМОШЕНКО

**Директор Центру забезпечення якості освіти
ПВНЗ «Європейський університет»
кандидат юридичних наук, доцент**



Олена КУЗЬМЕНКО



ЗАТВЕРДЖУЮ»

Директор
Тренінгового центру прокурорів
України

«04»  О. Отраднава 2025 р.

АКТ

**про впровадження в діяльність
Тренінгового центру прокурорів України
результатів дисертації Каланчі Інги Георгіївни
на тему: «Докази електронної форми в кримінальному процесі України:
теорія і практика» на здобуття наукового ступеня доктора юридичних наук зі
спеціальності 12.00.09 – кримінальний процес та криміналістика; судова
експертиза; оперативно-розшукова діяльність**

Комісія у складі:

Голови – заступника директора Тренінгового центру прокурорів України,
доктора юридичних наук, доцента А.М. Орлеана;

Членів комісії:

консультанта аналітичного відділу підготовки прокурорів Тренінгового центру
прокурорів України, доктора юридичних наук, професора
І.В. Берднік;

експерта аналітичного відділу підготовки прокурорів Тренінгового центру
прокурорів України, кандидата юридичних наук І.В. Пилипенка,

склала цей акт про те, що результати дисертаційного дослідження Каланчі Інги Георгіївни на тему: «Докази електронної форми в кримінальному процесі України: теорія і практика», поданої на здобуття наукового ступеня доктора юридичних наук зі спеціальності 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність, впроваджено в діяльність Тренінгового центру прокурорів України під час підвищення кваліфікації прокурорів з метою розвитку їх професійної компетенції щодо використання доказів, що мають електронну форму під час кримінального провадження.

Каланча Інга Георгіївна протягом 2021–2025 років провела 34 тренінги в Тренінговому центрі прокурорів України, зокрема:

- 1) 09.02.2021 проведено тренінг для прокурорів на тему: «Електронні (цифрові) докази» (офлайн, ТЦПУ);
- 2) 25.02.2021 проведено тренінг для прокурорів на тему: «Електронні (цифрові) докази» (офлайн, ТЦПУ);
- 3) 13.05.2021 проведено тренінг для прокурорів на тему: «Електронні (цифрові) докази» (офлайн, ТЦПУ);
- 4) 26.05.2021 проведено тренінг для прокурорів на тему: «Електронні (цифрові) докази» (офлайн, ТЦПУ);

5) 05.10.2021 проведено тренінг для прокурорів – стажистів окружної прокуратури на тему: «Робота з Єдиним реєстром досудових розслідувань» в межах програми первинної підготовки прокурорів – стажистів окружної прокуратури (онлайн);

6) 24.11.2021 проведено тренінг для прокурорів на тему: «Збирання та дослідження доказів у електронній формі під час кримінального провадження» (онлайн);

7) 25.11.2021 проведено тренінг для прокурорів на тему: «Аналіз та використання доказів у електронній формі під час кримінального провадження» (онлайн);

8) 15.12.2021 проведено тренінг для прокурорів на тему: «Збирання та дослідження доказів у електронній формі під час кримінального провадження» (офлайн, ТЦПУ);

9) 16.12.2021 проведено тренінг для прокурорів на тему: «Аналіз та використання доказів у електронній формі під час кримінального провадження» (офлайн, ТЦПУ);

10) 04.03.2022 проведено тренінг для прокурорів на тему: «Електронні докази» (онлайн);

11) 15.06.2022 проведено тренінг для прокурорів на тему: «Пошук, збирання і перевірка даних із відкритих джерел в інтернеті» (онлайн);

12) 17.06.2022 проведено тренінг для прокурорів на тему: «Фіксація даних з мережі „Інтернет“» (онлайн);

13) 18.07.2022 проведено тренінг для прокурорів на тему: «Пошук, збирання і перевірка даних із відкритих джерел в інтернеті» (онлайн);

14) 20.07.2022 проведено тренінг для прокурорів на тему: «Застосування механізму міжнародно-правової взаємодії при здійсненні фіксації інформації з інтернету» (онлайн);

15) 22.07.2022 проведено тренінг для прокурорів на тему: «Фіксація даних з мережі „Інтернет“» (онлайн);

16) 10.08.2022 проведено тренінг для прокурорів на тему: «Пошук, збирання і перевірка даних із відкритих джерел в інтернеті» (онлайн);

17) 09.09.2022 проведено тренінг для прокурорів на тему: «Фіксація даних з мережі „Інтернет“» (онлайн);

18) 25.01.2023 проведено тренінг для прокурорів на тему: «Пошук, збирання і перевірка даних із відкритих джерел в інтернеті» (онлайн);

19) 13.03.2023 проведено тренінг для прокурорів на тему: «Фіксація даних з мережі „Інтернет“» (онлайн);

20) 24.05.2023 проведено тренінг для прокурорів на тему: «Цифрові докази у кримінальному провадженні (день 1)» (офлайн, ТЦПУ);

21) 25.05.2023 проведено тренінг для прокурорів на тему: «Цифрові докази у кримінальному провадженні (день 2)» (офлайн, ТЦПУ);

22) 08.08.2023 проведено тренінг для прокурорів – стажистів окружної прокуратури на тему: «Робота прокурора в ІАС „ОСОП“» в межах програми первинної підготовки прокурорів – стажистів окружної прокуратури (офлайн, ТЦПУ);

23) 09.08.2023 проведено тренінг для прокурорів – стажистів окружної прокуратури на тему: «Основні засади ведення Єдиного реєстру досудових розслідувань» в межах програми первинної підготовки прокурорів – стажистів окружної прокуратури (офлайн, ТЦПУ);

24) 08.11.2023 проведено тренінг для прокурорів на тему: «Цифрові докази у кримінальному провадженні (день 1)» (офлайн, ТЦПУ);

25) 09.11.2023 проведено тренінг для прокурорів на тему: «Цифрові докази у кримінальному провадженні (день 2)» (офлайн, ТЦПУ);

26) 20.06.2024 проведено тренінг для прокурорів на тему: «Цифрові докази у кримінальному провадженні (день 1)» (офлайн, ТЦПУ);

27) 21.06.2024 проведено тренінг для прокурорів на тему: «Цифрові докази у кримінальному провадженні (день 2)» (офлайн, ТЦПУ);

28) 12.08.2024–13.08.2024 проведено тренінги для прокурорів – стажистів окружної прокуратури на тему: «Основні засади ведення Єдиного реєстру досудових розслідувань» в межах програми первинної підготовки прокурора – стажиста окружної прокуратури (офлайн, ТЦПУ);

29) 05.12.2024–06.12.2024 проведено дводенний тренінг для прокурорів на тему: «Цифрові докази у кримінальному провадженні» (офлайн, ТЦПУ);

30) 03.04.2025 проведено тренінг для прокурорів на тему: «Застосування процесуального та аналітичного функціоналу Єдиного реєстру досудових розслідувань у практичній діяльності прокурора. Робота в ІАС „ОСОП”» (онлайн);

31) 14.05.2025–16.05.2025 проведено триденний тренінг для прокурорів на тему: «Цифрові докази у кримінальному провадженні» (офлайн, ТЦПУ);

32) 17.06.2025 проведено тренінг для прокурорів на тему: «Процесуальне керівництво та підтримання публічного обвинувачення у кримінальних провадженнях щодо кіберзлочинів» (онлайн);

33) 19.06.2025 проведено тренінг для прокурорів на тему: «Процесуальне керівництво досудовим розслідуванням кримінальних правопорушень, вчинених із використанням криптовалюти» (онлайн);

34) 16.09.2025 проведено тренінг для прокурорів на тему: «Застосування процесуального та аналітичного функціоналів Єдиного реєстру досудових розслідувань у практичній діяльності прокурора. Робота прокурора в ІАС „ОСОП”» (онлайн).

Також Каланча Інга Георгіївна в жовтні 2022 року підготувала навчальний модуль «Електронні докази та пошук даних в мережі „Інтернет”» для Порталу дистанційного навчання ТЦПУ.

Як тренер ТЦПУ Каланча Інга Георгіївна 16.04.2024–21.06.2024 забезпечила проведення тьюторського курсу для прокурорів та суддів «Кіберзлочинність та електронні докази», організованого Тренінговим центром прокурорів України, Національною школою суддів України у співпраці з Радою Європи в межах проєкту HELP (Освіта в галузі прав людини для юристів) Ради Європи.

Також Каланча Інга Георгіївна як тренер ТЦПУ забезпечила проведення трьох тренінгів, організованих ТЦПУ у співпраці з Радою Європи в межах проєкту CyberUA «Зміцнення спроможності щодо електронних доказів воєнних злочинів і грубих порушень прав людини в Україні» Ради Європи, а саме:

1) 17.07.2024–18.07.2024 проведено дводенний тренінг для прокурорів та суддів на тему: «Допустимість, оброблення та ланцюг зберігання електронних доказів для прокурорів і суддів України» (офлайн, м. Київ);

2) 18.09.2024–19.09.2024 проведено дводенний тренінг для прокурорів на тему: «Допустимість, оброблення та ланцюг зберігання електронних доказів» (офлайн, м. Чернівці);

3) 19.11.2024–21.11.2024 проведено триденний тренінг для прокурорів, слідчих, детективів та оперативних працівників на тему: «Зберігання, виготовлення та оцінювання електронних доказів вчинення військових злочинів та грубих порушення прав людини (GHRV)» (офлайн, м. Львів).

Під час проведення вказаних тренінгів використано результати дисертаційного дослідження Каланчі Інги Георгіївни на тему: «Докази електронної форми в кримінальному процесі України: теорія і практика», що висвітлені у таких наукових публікаціях:

1) Patreliuk, D., Svoboda, I., Kalancha, I., Filashkin, V., Kachmar, B. Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations. *Pakistan Journal of Life and Social Sciences*, 2024, 22(2), pp. 4811–4820. DOI: <https://doi.org/10.57239/PJLSS-2024-22.2.00356>

2) Kozii, V.; Kalancha, I.; Vlasova, H.; Orlean, A. Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies. *IDP. Internet, Law and Politics Journal*, 2025, no. 42, pp. 1-13. DOI: <http://dx.doi.org/10.7238/idp.v0i42.429924> URL: <https://raco.cat/index.php/IDP/article/view/429924/526486>

3) Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Азербайджану. *Науковий вісник Ужгородського національного університету. Серія «Право»*. №59. 2019. С. 117-121. DOI: <https://doi.org/10.32782/2307-3322.59-2.26>

4) Каланча І.Г. Електронний сегмент кримінального процесу Естонії. *Порівняльно-аналітичне право*, №3, 2019. С. 212-216. URL: https://pap-journal.in.ua/wp-content/uploads/2021/07/3_2019.pdf

5) Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. № 146, 2019. С. 179-191. DOI: <https://doi.org/10.21564/2414-990x.146.171218>

6) Каланча І.Г. Електронний сегмент в кримінальному процесі Грузії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №4. 2019. С. 161-166. DOI: <https://doi.org/10.31733/2078-3566-2019-4-161-166>

7) Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Туркменістану. *Актуальні проблеми вітчизняної юриспруденції*. № 1. 2020. С. 91-95. DOI: <https://doi.org/10.15421/392021> URL: http://apnl.dnu.in.ua/1_2020/23.pdf

8) Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Вірменії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №1. 2020. С. 205-210. DOI: <https://doi.org/10.31733/2078-3566-2020-1-205-210>

- 9) Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Латвії. *Криміналістика і судова експертиза : міжвідомчий науково-методичний збірник*. Вип. 65, 2020. С. 90-100. DOI: <https://doi.org/10.33994/kndise.2020.65.09>
- 10) Каланча І.Г. Електронний сегмент в кримінальному процесуальному законодавстві Молдови. *Jurnalul Juridic National: teorie si practica*. №1 (41). 2020. С. 132-137. URL: <http://www.jurnaluljuridic.in.ua/archive/2020/1/30.pdf>
- 11) Каланча І.Г. Інтероперабельність як обов'язкова властивість електронних інформаційних систем органів кримінальної юстиції. *Ročenka Ukrajinsko-Slovenská. Zbornik vedeckých prác*. (Річник Українсько-Словацький. Збірник наукових праць) 2020. С. 64-70. URL: <https://www.eeda.sk/dok/publikacie/ostatne/2020-rocenka-ukrajinsko-slovenska.pdf>
- 12) Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*, №8, 2021. С. 336-339. DOI: <https://doi.org/10.32782/2524-0374/2021-8/77>
- 13) Каланча І.Г., Орлеан А.М. Адаптація системи кримінальної юстиції до цифровізації світу : роль навчального компоненту. *Наукові перспективи*, №11 (53), 2024. С. 937-944. DOI: [https://doi.org/10.52058/2708-7530-2024-11\(53\)-937-944](https://doi.org/10.52058/2708-7530-2024-11(53)-937-944)
- 14) Каланча І.Г., Юрчишин Ю.В. Забезпечення безпеки прокурора під час роботи з електронним сегментом кримінального провадження в Україні. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки*. Том 35 (74) № 6, 2024. С. 108-115. DOI: <https://doi.org/10.32782/TNU-2707-0581/2024.6/19>
- 15) Каланча І.Г. Алгоритм електронного кримінального провадження. *Law. State. Technology*, 2024. Вип. 4, С. 69–74. DOI: <https://doi.org/10.32782/LST/2024-4-13>
- 16) Каланча І.Г. Практика роботи з доказами, що мають електронну форму в кримінальному процесі України : соціологічне дослідження. *Успіхи і досягнення у науці*. №1(11), 2025, С. 76-93. DOI: [https://doi.org/10.52058/3041-1254-2025-1\(11\)-76-93](https://doi.org/10.52058/3041-1254-2025-1(11)-76-93)
- 17) Каланча І.Г., Стемковський Д.Б. Використання доказів, що мають електронну форму в кримінальному процесі України: судова практика. Аналітично-порівняльне правознавство. 2025. №2. С. 1001-1008. DOI <https://doi.org/10.24144/2788-6018.2025.02.148> <https://app-journal.in.ua/wp-content/uploads/2025/04/150.pdf>
- 18) Каланча І.Г. Електронний висновок експерта як доказ у кримінальному процесі України: практика, перспективи та ризики. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. №2. С. 84-92. DOI <https://doi.org/10.32782/2311-8040/2025-2-12> URL: <http://journals.lvduvs.lviv.ua/index.php/law/article/view/981/953>
- 19) Каланча І.Г. Процесуальна природа доказів, що мають електронну форму в кримінальному процесі України: документ та речовий доказ. *Міжнародний науковий журнал "Інтернаука". Серія: "Юридичні науки"*. № 7. 2025. DOI

<https://doi.org/10.25313/2520-2308-2025-7-11208> URL: <https://www.inter-nauka.com/issues/law2025/7/11208>

20) Каланча І.Г. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світлі концепції chain of custody. *Věda a perspektivy*. № 8(51) (2025). С. 206-230. URL: https://www.researchgate.net/publication/394998880_Kalanca_IG_Dokazi_so_maut_elektronnu_formu_v_kriminalnomu_procesi_Ukraini_identifikacia_ta_cilisnist_u_svitli_koncepcii_chain_of_custody_Veda_a_perspektivy_No_851_2025_C_206-230

21) Каланча І.Г. Єдине електронне інформаційне поле органів кримінальної юстиції. *Актуальні питання судової експертології, криміналістики та кримінального процесу*: мат. міжн. наук.-практ. конф. (м. Київ, 5.11.2019 р.). К., 2019. С. 209-213. URL: https://www.researchgate.net/publication/393743748_Kalanca_IG_Edine_elektronne_informacijne_pole_organiv_kriminalnoj_usticii_Aktualni_pitanna_sudovoi_ekspertologii_kriminalistiki_ta_kriminalnogo_procesu_mat_mizn_nauk-prakt_konf_m_Kiiv_5112019_r_K_2019

22) Каланча І.Г. Шляхи формування сучасних практичних компетентностей у випускників правничих шкіл України. *Інноваційні рішення в сучасній науці, освіті та практиці*: Матеріали I Міжнародної науково-практичної інтернет-конференції (наукове видання), 17-18 листопада 2020 р.: у 2 ч. Київ: НТУ, 2020. Ч.2. С. 209-212. URL: <http://vstup.ntu.edu.ua/conf-innov-part-2.pdf>

23) Гаркуша А.М., Каланча І.Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи*: матеріали круглого столу (м. Львів, 11 червня 2021 р.). Львів: Львівський державний університет внутрішніх справ, 2021. С. 159-165. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/11_06_2021.pdf

24) Каланча І.Г. Підходи до класифікації електронних носіїв інформації та інформаційних систем для завдань кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали V Міжнар. наук.-практ. конф. (29 жовтня 2021р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2021. С. 211-213. URL: <https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk-29.10.21.pdf>

25) Гаркуша А.М., Каланча І.Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. *Наукові читання пам'яті Ганса Гросса*: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівецький національний університет імені Юрія Федьковича. Чернівці: Технодрук, С. 72-75. URL:

http://dspace.unjvd.edu.ua/xmlui/bitstream/handle/123456789/11383/Forensic_Epistemology_Czernowitz_2021_.pdf?sequence=1&isAllowed=y

26) Каланча І.Г. Окремі аспекти діяльності прокурора щодо гарантування цілісності доказів, що мають електронну форму під час досудового розслідування кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VI Міжнар. наук.-практ. конф. (21 жовтня 2022р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2022. С. 327-332. URL:

https://ccu.gov.ua/sites/default/files/suchasni_vyklyky_ta_aktualni_problemy_sudovoi_reformy_v_ukrayini_2022.pdf

27) Каланча І.Г. Способи ідентифікації комп'ютерних даних як доказу в кримінальному провадженні. *III Наукові читання пам'яті Ганса Гросса* : збірник тез міжнародної науково-практичної конференції (м. Чернівці, 08 грудня 2023 р.). Чернівці: Чернівець. нац. У-нт. ім. Ю.Федьковича, 2023. С. 71-75. URL: <https://www.ndekc.cv.ua/wp-content/uploads/2024/03/III-Naukovi-chytannya-pam-yati-Gansa-Grossa.pdf>

28) Каланча І.Г. Стратегії фіксації доказів, що мають електронну форму для застосування в кримінальному провадженні. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VII Міжнар. наук.-практ. конф. (27 жовтня 2023р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2023. С. 253-258. URL: https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk_conf_27..pdf

29) Каланча І.Г. Кіберпростір як територія проведення досудового розслідування. *Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини*: зб. наук. праць за матер. Круглого столу, Київ, 7 грудня 2023 р. / редкол.: А.Ю. Нашинець-Наумова, Г.П. Власова, С.В. Бобровник, Т.О. Дідич, Н.А. Сергієнко, А.П. Чернега. – К. : Київ. стол. ун-т ім. Б. Грінченка, 2024. С. 115-119. URL: <https://kubg.edu.ua/struktura/pidrozdili/vurvdychna-klinika-astreya/zakhody/8438-ikh-kruhlyi-stil-prava-liudynv-v-umovakh-voiennoho-stanu-v-ukraini.html>

30) Каланча І.Г. Цифрова складова кримінального процесу України в науці та практиці: структурно-функціональний аналіз. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VIII Міжнар. наук.-практ. конф. (31 жовтня 2024р., Чернівці)/ редкол.: О.В. Щербанюк та ін. - Чернівці: 2024. С. 229-233. URL: https://www.researchgate.net/publication/390005117_Kalanca_IG_Cifrova_skladova_kriminalnogo_procesu_Ukraini_v_nauci_ta_praktici_strukturno-funkcionalnij_analiz_Sucasni_vikliki_ta_aktualni_problemi_sudovoi_reformi_v_Ukraini_Materiali_VIII_Miznar_nauk-p

31) Каланча І.Г. Результати OSINT як джерело доказів у кримінальному процесі України. *Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій*: Матеріали Всеукр. наук.-практ. конф. (м. Чернівці, 20 грудня 2024 р.) / відп. ред. К.А. Возняковська. ТОМ 1, Чернівці, 2024. С. 43-49. URL: https://www.researchgate.net/publication/389647938_Kalanca_IG_Rezultati_OSINT_ak_dzerele_dokaziv_u_kriminalnomu_procesi_Ukraini_Innovacii_vikliki_ta_novi_gorizon_ti_pravovogo_reguluvanna_u_svitli_sucasnih_socialno-ekonomichnih_ta_politichnih_transformaci

32) Каланча І.Г. Використання висновку експерта, що має електронну форму як доказу в кримінальному процесі України. *Актуальні проблеми національного законодавства*: збірник матеріалів Міжнародної науково-практичної конференції, м. Кропивницький, 17 квітня 2025 року. Частина 1. Кропивницький, 2025. С. 154-156. URL: https://www.researchgate.net/publication/392901845_Kalanca_IG_Vikoristanna_visnov

ku eksperta so mae elektronnu formu ak dokazu v kriminalnomu procesi Ukraini
Aktualni problemi nacionalnogo zakonodavstva zbirnik materialiv Miznarodnoi nau
kovo-prakticno

33) Каланча І. Термінологічне розмежування понять «електронний доказ», «цифровий доказ» і «доказ, що має електронну форму» в кримінальному процесі України. *Пріоритетні шляхи розвитку науки і освіти*: матеріали XV Міжнародної науково-практичної конференції м. Львів, 9-10 травня 2025 року. – Львів : Львівський науковий форум, 2025. С. 195-197. URL: <http://www.lviv-forum.inf.ua/save/2025/9-10.05/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA.pdf>

Відтак, вищезазначені матеріали Каланчі І.Г. можуть застосовуватися під час підвищення кваліфікації прокурорів з метою розвитку професійної компетенції щодо використання доказів, що мають електронну форму під час кримінального провадження.

Голова комісії:

заступник
 директора Тренінгового центру
 прокурорів України,
 доктор юридичних наук, доцент



А.М. Орлеан

Члени комісії:

консультант
 аналітичного відділу
 підготовки прокурорів
 Тренінгового центру
 прокурорів України,
 доктор юридичних наук, професор



І.В. Берднік

експерт
 аналітичного відділу
 підготовки прокурорів
 Тренінгового центру
 прокурорів України,
 кандидат юридичних наук



І.В. Пилипенко



RECOMMENDATION LETTER

I am writing to recommend **Inha Kalancha**, who served as a tutor for the HELP tutored course "Cybercrime and Electronic Evidence", organised by the Council of Europe Project "HELP (Human Rights Education for Legal Professionals) for Ukraine including during wartime" in collaboration with the Prosecutor's Training Centre of Ukraine and the National School of Judges of Ukraine. The course ran from 16 April to 21 June 2024, and targeted both judges and prosecutors.

In her dual role as a prosecutor and a representative of the Prosecutor's Training Centre of Ukraine, Ms. Kalancha played a pivotal role in preparing and delivering materials on the use of digital evidence in criminal proceedings, specifically tailored to the Ukrainian legal context. Her contributions ensured that the course content was both relevant and practical for legal professionals in Ukraine.

Throughout the course, Ms. Kalancha consistently demonstrated exceptional expertise and an impressive ability to engage participants, both in face-to-face and online formats. Her clear communication and practical experience greatly enriched the learning experience for all course participants.

Furthermore, her efforts resulted in the development of national adaptation materials for the HELP course on "Cybercrime and Electronic Evidence", which are now publicly accessible on the Council of Europe HELP online platform, extending the course's impact even further.

The national adaptation of the course can be accessed here: <https://help.elearning.ext.coe.int/course/view.php?id=5960>

Ms. Kalancha's professionalism, dedication, and subject-matter expertise make her an invaluable asset to any legal education initiative. I am confident that her continued contributions will significantly enhance the capacity of legal professionals in Ukraine and beyond.

International Manager of the Project
"HELP (Human Rights Education for Legal
Professionals) for Ukraine including during
wartime"

Olga KOSTENKO

Contact information: olga.kostenko@coe.int

16.10.2024



№ 3769_051_2025
Kyiv, Ukraine

October 30, 2025

RECOMMENDATION LETTER

Dear Sirs and Madams,

I work as Project Manager of the Council of Europe project “CyberUA: Strengthening capacities on electronic evidence of war crimes and gross human rights violations in Ukraine” (hereinafter – CyberUA).

The main objective of the CyberUA project is to enhance the capacity of Ukrainian law enforcement authorities, prosecutors, and the judiciary in the collection, preservation, analysis and handling electronic evidence for use in criminal proceedings related to war crimes and gross human rights violations (GHRV) committed in the context of the Russian war of aggression against Ukraine.

Ms. Inha Kalancha has been one of the national experts of the CyberUA project since its launch in 2024. Throughout 2025, Ms. Kalancha made substantial contributions by delivering the following capacity-building activities for project beneficiaries:

- Policy discussion on admissibility, processing and chain of custody concerning electronic evidence / Roundtable on electronic evidence in criminal procedure of Ukraine, during 28–29 January 2025 in Kyiv, Ukraine;
- Training on admissibility, processing and chain of custody of e-evidence for prosecutors and judges, during 12–13 March 2025 in Lviv, Ukraine;
- Introduction to electronic evidence of war crimes and related offences for media and civil society of Ukraine, Kyiv, Ukraine 17–19, March 2025;
- Workshop on legal reforms in compliance with requirements of the Budapest Convention on cybercrime and the Second Additional Protocol to the Budapest Convention, on 24–25 April 2025, in Uzhhorod, Ukraine;
- Policy discussion on admissibility, processing and chain of custody concerning electronic evidence in Ukraine, between 11–12 June 2025, in Lviv, Ukraine;
- Training course on preservation, production and analysis of data from different sources, between 09–11 September 2025, in Chernivtsi, Ukraine;
- Training on the substantive law elements of the crime of aggression, between 27–28 October 2025, in Lviv, Ukraine.

Ms. Kalancha has consistently demonstrated exceptional skill and professionalism in establishing national standards for collecting, handling and using electronic evidence in criminal proceedings. She focuses particularly on ensuring that such evidence remains reliable and legally admissible.

I have great respect for her work. Her extensive expertise, strong analytical abilities, and forward-thinking perspective will undoubtedly continue to enhance national legislation, policy frameworks, and practical procedures in this field.

I am pleased to recommend Ms. Kalancha as a highly competent and trusted specialist in the area of

electronic evidence in criminal proceedings.

Should you require any further information, please do not hesitate to contact me - iryna.laba@coe.int.

Best regards,

Iryna LABA
Project manager CyberUA
Cybercrime Division
Council of Europe - Conseil de l'Europe



30.10.2025

ЗАТВЕРДЖУЮ

Проректор Національної
академії внутрішніх справ
доктор юридичних наук, професор
полковник поліції

Сергій ЧЕРНЯВСЬКИЙ

2025 року

АКТ

10.07.2025

м. Київ

№ 125-оп

Впровадження результатів дисертації
Каланчі Інги Георгіївни на тему «Докази
електронної форми у кримінальному процесі
України: теорія та практика» в освітній
процес НАВС

Уклала експертна комісія з виявлення, узагальнення та впровадження
позитивного досвіду роботи у складі:

- т.в.о. заступника начальника відділу організації освітнього процесу,
кандидата юридичних наук, майора поліції Бистрицького Богдана Юрійовича;
- т.в.о. начальника відділу організації наукової діяльності, кандидата
юридичних наук старшого лейтенанта поліції Горбенко Дар'ї Андріївни;
- начальника відділу аспірантури (ад'юнктури) і докторантури, доктора
юридичних наук, професора підполковника поліції Тихонової Олени Вікторівни;
- завідувача кафедри кримінального процесу, доктора юридичних наук,
професора підполковника поліції Таран Олени Вікторівни;
- завідувача загальної бібліотеки Гайдар Людмили Георгіївни.

Комісія розглянула й узагальнила наукові праці здобувачки кафедри
кримінального процесу Національної академії внутрішніх Каланчі Інги Георгіївни
на тему «Докази електронної форми у кримінальному процесі України: теорія та
практика» поданої на здобуття наукового ступеня доктора юридичних наук зі
спеціальності 12.00.09 – кримінальний процес та криміналістика; судова
експертиза; оперативно-розшукова діяльність.

Проаналізовано основні результати дослідження Каланчі І.Г., зокрема наукові
праці, в яких опубліковані теоретичні положення дисертації:

Каланча І.Г. Практика роботи з доказами, що мають електронну форму в
кримінальному процесі України : соціологічне дослідження. *Успіхи і досягнення у
науці*. №1(11). 2025. С. 76-93. DOI: [https://doi.org/10.52058/3041-1254-2025-1\(11\)-76-93](https://doi.org/10.52058/3041-1254-2025-1(11)-76-93)

Каланча І.Г. Електронний висновок експерта як доказ у кримінальному
процесі України: практика, перспективи та ризики. *Науковий вісник Львівського
державного університету внутрішніх справ (серія юридична)*. 2025. №2. С. 84-92.
DOI <https://doi.org/10.32782/2311-8040/2025-2-12>

Каланча І.Г., Стемковський Д.Б. Використання доказів, що мають електронну форму в кримінальному процесі України: судова практика. Аналітично-порівняльне правознавство. 2025. №2. С. 1001-1008. DOI <https://doi.org/10.24144/2788-6018.2025.02.148> <https://app-journal.in.ua/wp-content/uploads/2025/04/150.pdf>

Kozii, V.; Kalancha, I.; Vlasova, H.; Orlean, A. Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies. *IDP. Internet, Law an Politics Journal*, 2025, no. 42. DOI: <http://dx.doi.org/10.7238/idp.v0i42.429924> URL: <https://raco.cat/index.php/IDP/article/view/429924/526486>

Каланча І.Г. Результати OSINT як джерело доказів у кримінальному процесі України. *Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій*: Матеріали Всеукр. наук.-практ. конф. (м. Чернівці, 20 грудня 2024 р.) / відп. ред. К.А. Возняковська. ТОМ 1, Чернівці, 2024. С. 43-49. URL: https://www.researchgate.net/publication/389647938_Kalanca_IG_Rezultati_OSINT_ak_dzerelo_dokaziv_u_kriminalnomu_procesi_Ukraini_Innovacii_vikliki_ta_novi_gorizon_ti_pravovogo_reguluvanna_u_svitli_sucasnih_socialno-ekonomichnih_ta_politichnih_transformaci

Каланча І. Термінологічне розмежування понять «електронний доказ», «цифровий доказ» і «доказ, що має електронну форму» в кримінальному процесі України. *Пріоритетні шляхи розвитку науки і освіти*: матеріали XV Міжнародної науково-практичної конференції м. Львів, 9-10 травня 2025 року. – Львів : Львівський науковий форум, 2025. С. 195-197. URL: <http://www.lviv-forum.inf.ua/save/2025/9-10.05/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA.pdf>

Каланча І.Г. Використання висновку експерта, що має електронну форму як доказу в кримінальному процесі України. Актуальні проблеми національного законодавства: збірник матеріалів Міжнародної науково-практичної конференції, м. Кропивницький, 17 квітня 2025 року. Частина 1. Кропивницький, 2025. С. 154-156. URL: https://www.researchgate.net/publication/392901845_Kalanca_IG_Vikoristanna_visnovku_eksperta_so_mae_elektronnu_formu_ak_dokazu_v_kriminalnomu_procesi_Ukraini_Aktualni_problemi_nacionalnogo_zakonodavstva_zbirnik_materialiv_Miznarodnoi_naukovo-prakticno

Patreliuk, D., Svoboda, I., Kalancha, I., Filashkin, V., Kachmar, B. Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations. *Pakistan Journal of Life and Social Sciences*, 2024, 22(2), pp. 4811–4820. DOI: <https://doi.org/10.57239/PJLSS-2024-22.2.00356> Scopus ID: 59332866200

Каланча І.Г. Алгоритм електронного кримінального провадження. *Law. State. Technology*, 2024. Вип. 4, С. 69–74. DOI: <https://doi.org/10.32782/LST/2024-4-13>

Каланча І.Г., Юрчишин Ю.В. Забезпечення безпеки прокурора під час роботи з електронним сегментом кримінального провадження в Україні. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки*. Том 35 (74) № 6, 2024. С. 108-115. DOI: <https://doi.org/10.32782/TNU-2707-0581/2024.6/19>

Каланча І.Г., Орлеан А.М. Адаптація системи кримінальної юстиції до цифровізації світу : роль навчального компоненту. *Наукові перспективи*, №11 (53), 2024. С. 937-944. DOI: [https://doi.org/10.52058/2708-7530-2024-11\(53\)-937-944](https://doi.org/10.52058/2708-7530-2024-11(53)-937-944)

Каланча І.Г. Цифрова складова кримінального процесу України в науці та практиці: структурно-функціональний аналіз. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VIII Міжнар. наук.-практ. конф. (31 жовтня 2024р., Чернівці)/ редкол.: О.В. Щербанюк та ін. - Чернівці: 2024. С. 229-233. URL:

https://www.researchgate.net/publication/390005117_Kalanca_IG_Cifrova_skladova_kriminalnogo_procesu_Ukraini_v_nauci_ta_praktici_strukturno-funkcionalnij_analiz_Sucasni_vikliki_ta_aktualni_problemi_sudovoi_reformi_v_Ukraini_Materiali_VIII_Miznar_nauk-p

Каланча І.Г. Способи ідентифікації комп'ютерних даних як доказу в кримінальному провадженні. *III Наукові читання пам'яті Ганса Гросса* : збірник тез міжнародної науково-практичної конференції (м. Чернівці, 08 грудня 2023 р.). Чернівці: Чернівець. нац. У-нт. ім. Ю.Федьковича, 2023. С. 71-75. URL: <https://www.ndekc.cv.ua/wp-content/uploads/2024/03/III-Naukovi-chytannya-pam-yati-Gansa-Grossa.pdf>

Каланча І.Г. Кіберпростір як територія проведення досудового розслідування. *Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини*: зб. наук. праць за матер. Круглого столу, Київ, 7 грудня 2023 р. / редкол.: А.Ю. Нашинець-Наумова, Г.П. Власова, С.В. Бобровник, Т.О. Дідич, Н.А. Сергієнко, А.П. Чернега. – К. : Київ. стол. ун-т ім. Б. Грінченка, 2024. С. 115-119. URL: <https://kubg.edu.ua/struktura/pidrozdzili/yurydychna-klinika-astreya/zakhody/8438-ikh-kruhlyi-stil-prava-liudyny-v-umovakh-voiennoho-stanu-v-ukraini.html>

Каланча І.Г. Стратегії фіксації доказів, що мають електронну форму для застосування в кримінальному провадженні. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VII Міжнар. наук.-практ. конф. (27 жовтня 2023р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2023. С. 253-258. URL: https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk_conf_27..pdf

Каланча І.Г. Окремі аспекти діяльності прокурора щодо гарантування цілісності доказів, що мають електронну форму під час досудового розслідування кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VI Міжнар. наук.-практ. конф. (21 жовтня 2022р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2022. С. 327-332. URL: https://ccu.gov.ua/sites/default/files/suchasni_vyklyky_ta_aktualni_problemy_sudovoyi_reformy_v_ukrayini_2022.pdf

Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*, №8, 2021. С. 336-339. DOI: <https://doi.org/10.32782/2524-0374/2021-8/77>

Гаркуша А.М., Каланча І.Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. *Наукові читання пам'яті Ганса Гросса*: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівецький

національний університет імені Юрія Федьковича. Чернівці : Технодрук, С. 72-75. URL:

http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/11383/Forensic_Epistemology_Czernowitz_2021_.pdf?sequence=1&isAllowed=y

Каланча І.Г. Підходи до класифікації електронних носіїв інформації та інформаційних систем для завдань кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали V Міжнар. наук.-практ. конф. (29 жовтня 2021р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2021. С. 211-213. URL: <https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk-29.10.21.pdf>

Таркуша А.М., Каланча І.Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи*: матеріали круглого столу (м. Львів, 11 червня 2021 р.). Львів: Львівський державний університет внутрішніх справ, 2021. С. 159-165. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/11_06_2021.pdf

Каланча І.Г. Інтероперабельність як обов'язкова властивість електронних інформаційних систем органів кримінальної юстиції. *Ročenka Ukrajinsko-Slovenská. Zborník vedeckých prác*. (Рочник Українсько-Словацький. Збірник наукових праць) 2020. С. 64-70. URL: <https://www.eeda.sk/dok/publikacie/ostatne/2020-rocenka-ukrajinsko-slovenska.pdf>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законодавстві Молдови. *Jurnalul Juridic National: teorie si practica*. №1 (41). 2020. С. 132-137. URL: <http://www.jurnaluljuridic.in.ua/archive/2020/1/30.pdf>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Латвії. *Криміналістика і судова експертиза : міжвідомчий науково-методичний збірник*. Вип. 65, 2020. С. 90-100. DOI: <https://doi.org/10.33994/kndise.2020.65.09>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Вірменії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №1. 2020. С. 205-210. DOI: <https://doi.org/10.31733/2078-3566-2020-1-205-210>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Туркменістану. *Актуальні проблеми вітчизняної юриспруденції*. № 1. 2020. С. 91-95. DOI: <https://doi.org/10.15421/392021> URL: http://apnl.dnu.in.ua/1_2020/23.pdf

Каланча І.Г. Поняття практики Європейського суду з прав людини як джерела кримінального процесуального права України. *Вісник кримінального судочинства*, № 2, 2020, С. 8-21. URL: https://vkslaw.knu.ua/images/verstka/Visnyk_Krim_Sud_3-4_20_231013_avt-8-21.pdf

Каланча І.Г. Тенденції та динаміка застосування практики Європейського суду з прав людини під час кримінального провадження: статистичне та соціологічне дослідження. *Теорія і практика правознавства*, Вип. 2(18), 2020. С. 14 (1-17). DOI: <https://doi.org/10.21564/2225-6555.2020.18.213676>

Каланча І.Г. Роль правових актів Європейського суду з прав людини в кримінальному процесі України. *Проблеми законності : зб. наук. праць*. № 150, 2020. С. 233-243. DOI: <https://doi.org/10.21564/2414-990x.150.209071>

Каланча І.Г. Шляхи формування сучасних практичних компетентностей у випускників правничих шкіл України. *Інноваційні рішення в сучасній науці*,

освіті та практиці: Матеріали I Міжнародної науково-практичної інтернет-конференції (наукове видання), 17-18 листопада 2020 р.: у 2 ч. Київ: НТУ, 2020. Ч.2. С. 209-212. URL: <http://vstup.ntu.edu.ua/conf-innov-part-2.pdf>

Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. № 146, 2019. С. 179-191. DOI: <https://doi.org/10.21564/2414-990x.146.171218>

Каланча І.Г. Електронний сегмент в кримінальному процесі Грузії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №4. 2019. С. 161-166. DOI: <https://doi.org/10.31733/2078-3566-2019-4-161-166>

Каланча І.Г. Електронний сегмент кримінального процесу Естонії. *Порівняльно-аналітичне право*, №3, 2019. С. 212-216. URL: https://pap-journal.in.ua/wp-content/uploads/2021/07/3_2019.pdf

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Азербайджану. *Науковий вісник Ужгородського національного університету. Серія «Право»*. №59. 2019. С. 117-121. DOI: <https://doi.org/10.32782/2307-3322.59-2.26>

Каланча І.Г. Єдине електронне інформаційне поле органів кримінальної юстиції. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : мат. міжн. наук.-практ. конф. (м. Київ, 5.11.2019 р.). К., 2019. С. 209-213. URL: https://www.researchgate.net/publication/393743748_Kalanca_IG_Edine_elektronne_in_formacijne_pole_organiv_kriminalnoi_usticii_Aktualni_pitanna_sudovoi_ekspertologii_kriminalistiki_ta_kriminalnogo_procesu_mat_mizn_nauk-prakt_konf_m_Kiiv_5112019_r_K_2019

На основі проведеного аналізу комісія зробила висновок, що праці Каланчі І.Г. містять науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання в освітньому процесі Національної академії внутрішніх справ, зокрема при викладанні навчальних дисциплін «Кримінальний процес», «Практика Європейського суду з прав людини у кримінальному провадженні», «Процесуальні документи в кримінальному провадженні», «Складання процесуальних документів на стадії досудового розслідування», під час підготовки навчально-методичних та дидактичних матеріалів, а також рекомендувати їх до вивчення під час самостійної роботи здобувачів вищої освіти.

Члени комісії:

 **Богдан БИСТРИЦЬКИЙ**

 **Дар'я ГОРБЕНКО**

 **Олена ТИХОНОВА**

 **Олена ТАРАН**

 **Людмила ГАЙДАР**

ЗАТВЕРДЖУЮ

Заступник декана факультету
права та міжнародних відносин
Київського столичного університету
імені Бориса Грінченка
доктор юридичних наук, професор



Лілія НАШИНЕЦЬ-НАУМОВА

Лілія 2025 року

АКТ

«___» _____ 2025 року

м. Київ

про впровадження результатів
дисертаційного дослідження Каланчі Інги
Георгіївни на тему: «Докази електронної
форми в кримінальному процесі України:
теорія і практика» у освітній процес
Київського столичного університету імені
Бориса Грінченка

Комісія у складі:

завідувача кафедри публічного права факультету права та міжнародних відносин Київського столичного університету імені Бориса Грінченка, доктора юридичних наук, професора, заслуженого діяча науки і техніки України Цимбал Ганни Петрівни,

професора кафедри публічного права факультету права та міжнародних відносин Київського столичного університету імені Бориса Грінченка, доктора юридичних наук, доцента Завидника Володимира Івановича,

доцента кафедри публічного права факультету права та міжнародних відносин Київського столичного університету імені Бориса Грінченка, доктора філософії в галузі права Лісіцького Андрія Валерійовича,

розглянула й узагальнила результати дисертаційного дослідження здобувачки кафедри кримінального процесу Національної академії внутрішніх справ Каланчі Інги Георгіївни на тему: «Докази електронної форми у кримінальному процесі України: теорія та практика», поданого на здобуття наукового ступеня доктора юридичних наук зі спеціальності 12.00.09 - кримінальний процес та криміналістика; судова експертиза; оперативно-

розшукова діяльність. На основі проведеного аналізу комісія зробила висновок, що надані наукові праці містять низку обґрунтованих теоретичних положень і пропозицій, спрямованих на теоретичне дослідження доказів електронної форми у кримінальному процесі України.

Проаналізовано основні результати дослідження Каланчі І.Г., зокрема наукові праці, в яких опубліковані положення дисертаційного дослідження:

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Азербайджану. *Науковий вісник Ужгородського національного університету. Серія «Право»*. №59. 2019. С. 117-121. DOI: <https://doi.org/10.32782/2307-3322.59-2.26>

Каланча І.Г. Електронний сегмент кримінального процесу Естонії. *Порівняльно-аналітичне право*, №3, 2019. С.212-216. URL: https://pap-journal.in.ua/wp-content/uploads/2021/07/3_2019.pdf

Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. № 146, 2019. С. 179-191. DOI: <https://doi.org/10.21564/2414-990x.146.171218>

Каланча І.Г. Електронний сегмент в кримінальному процесі Грузії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №4. 2019. С. 161-166. DOI: <https://doi.org/10.31733/2078-3566-2019-4-161-166>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законодавстві Молдови. *Jurnalul Juridic National: teorie si practica*. №1 (41). 2020. С. 132-137. URL: <http://www.jurnaluljuridic.in.ua/archive/2020/1/30.pdf>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Туркменістану. *Актуальні проблеми вітчизняної юриспруденції*. № 1. 2020. С. 91-95. DOI: <https://doi.org/10.15421/392021> URL: http://apnl.dnu.in.ua/1_2020/23.pdf

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Вірменії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №1. 2020. С. 205-210. DOI: <https://doi.org/10.31733/2078-3566-2020-1-205-210>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Латвії. *Криміналістика і судова експертиза : міжвідомчий науково-методичний збірник*. Вип. 65, 2020. С. 90-100. DOI: <https://doi.org/10.33994/kndise.2020.65.09>

Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*, №8, 2021. С. 336-339. DOI: <https://doi.org/10.32782/2524-0374/2021-8/77>

Patreliuk, D., Svoboda, I., Kalancha, I., Filashkin, V., Kachmar, B. Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations. *Pakistan Journal of Life and Social Sciences*, 2024, 22(2), pp. 4811–4820. DOI: <https://doi.org/10.57239/PJLSS-2024-22.2.00356>

Каланча І.Г., Орлеан А.М. Адаптація системи кримінальної юстиції до цифровізації світу : роль навчального компоненту. *Наукові перспективи*, №11 (53), 2024. С. 937-944. DOI: [https://doi.org/10.52058/2708-7530-2024-11\(53\)-937-944](https://doi.org/10.52058/2708-7530-2024-11(53)-937-944)

Каланча І.Г., Юрчишин Ю.В. Забезпечення безпеки прокурора під час роботи з електронним сегментом кримінального провадження в Україні. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки*. Том 35 (74) № 6, 2024. С. 108-115. DOI: <https://doi.org/10.32782/TNU-2707-0581/2024.6/19>

Каланча І.Г. Алгоритм електронного кримінального провадження. *Law. State. Technology*, 2024. Вип. 4, С. 69–74. DOI: <https://doi.org/10.32782/LST/2024-4-13>

Каланча І.Г. Практика роботи з доказами, що мають електронну форму в кримінальному процесі України : соціологічне дослідження. *Успіхи і досягнення у науці*. №1(11). 2025. С. 76-93. DOI: [https://doi.org/10.52058/3041-1254-2025-1\(11\)-76-93](https://doi.org/10.52058/3041-1254-2025-1(11)-76-93)

Каланча І.Г., Стемковський Д.Б. Використання доказів, що мають електронну форму в кримінальному процесі України: судова практика. Аналітично-порівняльне правознавство. 2025. №2. С. 1001-1008. DOI: <https://doi.org/10.24144/2788-6018.2025.02.148> <https://app-journal.in.ua/wp-content/uploads/2025/04/150.pdf>

Каланча І.Г. Електронний висновок експерта як доказ у кримінальному процесі України: практика, перспективи та ризики. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. №2. С. 84-92. DOI: <https://doi.org/10.32782/2311-8040/2025-2-12> URL: <http://journals.lvduvs.lviv.ua/index.php/law/article/view/981/953>

Каланча І.Г. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світлі концепції chain of custody. *Věda a perspektivy*. № 8(51) (2025). С. 206-230. URL: https://www.researchgate.net/publication/394998880_Kalanca_IG_Dokazi_so_maut_elektronnu_formu_v_kriminalnomu_procesi_Ukraini_identifikacia_ta_cilisni_st_u_svitli_koncepcii_chain_of_custody_Veda_a_perspektivy_No_851_2025_C_206-230

Kozii, V.; Kalancha, I.; Vlasova, H.; Orlean, A. Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies. *IDP. Internet, Law an Politics Journal*, 2025, no. 42. pp. 1-

13. DOI: <http://dx.doi.org/10.7238/idp.v0i42.429924> URL: <https://raco.cat/index.php/IDP/article/view/429924/526486>

Каланча І.Г. Процесуальна природа доказів, що мають електронну форму в кримінальному процесі України: документ та речовий доказ. *Міжнародний науковий журнал "Інтернаука". Серія: "Юридичні науки"*. № 7. 2025. С. 85-92. DOI <https://doi.org/10.25313/2520-2308-2025-7-11208> URL: <https://www.inter-nauka.com/uploads/public/17557614844770.pdf>

Каланча І.Г. Організаційні аспекти роботи з доказами, що мають електронну форму в кримінальному процесі України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. Вип. 90, Ч. 4. 2025. С. 258-266. DOI <https://doi.org/10.24144/2307-3322.2025.90.4.36>

Каланча І.Г. Єдине електронне інформаційне поле органів кримінальної юстиції. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : мат. міжн. наук.-практ. конф. (м. Київ, 5.11.2019 р.). К., 2019. С. 209-213. URL: https://www.researchgate.net/publication/393743748_Kalanca_IG_Edine_elektronne_informacijne_pole_organiv_kriminalnoi_usticii_Aktualni_pitannya_sudovoi_eksptologiji_kriminalistiki_ta_kriminalnogo_procesu_mat_mizn_nauk-prakt_konf_m_Kiiv_5112019_r_K_2019

Каланча І.Г. Шляхи формування сучасних практичних компетентностей у випускників правничих шкіл України. *Інноваційні рішення в сучасній науці, освіті та практиці*: Матеріали I Міжнародної науково-практичної інтернет-конференції (наукове видання), 17-18 листопада 2020 р.: у 2 ч. Київ: НТУ, 2020. Ч.2. С. 209-212. URL: <http://vstup.ntu.edu.ua/conf-innov-part-2.pdf>

Гаркуша А.М., Каланча І.Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи*: матеріали круглого столу (м. Львів, 11 червня 2021 р.). Львів: Львівський державний університет внутрішніх справ., 2021. С. 159-165. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/11_06_2021.pdf

Каланча І.Г. Підходи до класифікації електронних носіїв інформації та інформаційних систем для завдань кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали V Міжнар. наук.-практ. конф. (29 жовтня 2021р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2021. С. 211-213. URL: <https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk-29.10.21.pdf>

Гаркуша А.М., Каланча І.Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. *Наукові читання пам'яті Ганса Гросса*: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівецький національний університет імені Юрія Федьковича. Чернівці : Технодрук, С.

72-75.

URL:

http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/11383/Forensic_Epi-stemology_Czernowitz_2021_.pdf?sequence=1&isAllowed=y

Каланча І.Г. Окремі аспекти діяльності прокурора щодо гарантування цілісності доказів, що мають електронну форму під час досудового розслідування кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VI Міжнар. наук.-практ. конф. (21 жовтня 2022р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2022. С. 327-332.

URL:

https://ccu.gov.ua/sites/default/files/suchasni_vyklyky_ta_aktualni_problemy_sudovoi_reformy_v_ukrayini_2022.pdf

Каланча І.Г. Способи ідентифікації комп'ютерних даних як доказу в кримінальному провадженні. *III Наукові читання пам'яті Ганса Гросса*: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 08 грудня 2023 р.). Чернівці: Чернівець. нац. У-нт. ім. Ю.Федьковича, 2023. С. 71-75. URL: <https://www.ndekc.cv.ua/wp-content/uploads/2024/03/III-Naukovi-chytannya-pam-yati-Gansa-Grossa.pdf>

Каланча І.Г. Стратегії фіксації доказів, що мають електронну форму для застосування в кримінальному провадженні. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VII Міжнар. наук.-практ. конф. (27 жовтня 2023р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2023. С. 253-258. URL: https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk_conf_27_.pdf

Каланча І.Г. Кіберпростір як територія проведення досудового розслідування. *Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини*: зб. наук. праць за матер. Круглого столу, Київ, 7 грудня 2023 р. / редкол.: А.Ю. Нашинєць-Наумова, Г.П. Власова, С.В. Бобровник, Т.О. Дідич, Н.А. Сергієнко, А.П. Чернега. – К.: Київ. стол. ун-т ім. Б. Грінченка, 2024. С. 115-119. URL: <https://kubg.edu.ua/struktura/pidrozdili/yurydychna-klinika-astreya/zakhody/8438-ikh-kruhlyi-stil-prava-liudyny-v-umovakh-voiennoho-stanu-v-ukraini.html>

Каланча І.Г. Цифрова складова кримінального процесу України в науці та практиці: структурно-функціональний аналіз. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VIII Міжнар. наук.-практ. конф. (31 жовтня 2024р., Чернівці)/ редкол.: О.В. Щербанюк та ін. - Чернівці: 2024. С. 229-233. URL: https://www.researchgate.net/publication/390005117_Kalanca_IG_Cifrova_sklado_va_kriminalnogo_procesu_Ukraini_v_nauci_ta_praktici_strukturno-funkcionalnij_analiz_Suchasni_viklyki_ta_aktualni_problemi_sudovoi_reformi_v_Ukraini_Materiali_VIII_Miznar_nauk-p

Каланча І.Г. Матеріальна форма існування як властивість доказу в кримінальному процесі України: практика правозастосування. *Права людини*

в умовах воєнного стану в Україні: Х круглий стіл до Всеукраїнського тижня права (10 грудня 2024 року). *Права людини в умовах воєнного стану в Україні: до тижня права і Загальної декларації прав людини* : зб. наук. праць за матер. круглого столу, Київ, 10 грудня 2024 р. / редкол.: А.Ю. Нашинець-Наумова, Г.П. Цимбал, С.В. Бобровник, Т.О. Дідич, О.І. Чаплук, А.П. Чернега. — Київ : Київ. столич. ун-т ім. Б. Грінченка, 2025. С. 63-67. URL: https://www.researchgate.net/publication/396154856_Kalanca_IG_Materialna_forma_isnuvanna_ak_vlastivist_dokazu_v_kriminalnomu_procesi_Ukraini_praktika_pravozastosuvannya_Prava_ludini_v_umovah_voennogo_stanu_v_Ukraini_X_kruglij_stil_do_Vseukrainskogo_tiz

Каланча І. Термінологічне розмежування понять «електронний доказ», «цифровий доказ» і «доказ, що має електронну форму» в кримінальному процесі України. *Пріоритетні шляхи розвитку науки і освіти: матеріали XV Міжнародної науково-практичної конференції* м. Львів, 9-10 травня 2025 року. — Львів : Львівський науковий форум, 2025. С. 195-197. URL: <http://www.lviv-forum.inf.ua/save/2025/9-10.05/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA.pdf>

Власова Г.П., Каланча І.Г. Захисник як суб'єкт роботи з електронними доказами в кримінальному провадженні. *Актуальні питання реформування правової системи* : зб. матеріалів ХХІІ Міжнар. наук.-практ. конф., Луцьк, 13-15 червня 2025 р. / Уклад. Джурак Л. М. — Луцьк : Вежа-Друк, 2025. С. 113-115. URL: https://www.law.vnu.edu.ua/_files/ugd/65dd18_5ab2de833d004115b0483aa2420d7cc0.pdf

Каланча І.Г. Результати OSINT як джерело доказів у кримінальному процесі України. *Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій: Матеріали Всеукр. наук.-практ. конф. (м. Чернівці, 20 грудня 2024 р.)* / відп. ред. К.А. Возняковська. ТОМ 1, Чернівці, 2024. С. 43-49. URL: https://www.researchgate.net/publication/389647938_Kalanca_IG_Rezultati_OSINT_ak_dzerele_dokaziv_u_kriminalnomu_procesi_Ukraini_Innovacii_vikliki_ta_novi_gorizonti_pravovogo_reguluvannya_u_svitli_sucasnih_socialno-ekonomichnih_ta_politichnih_transformaci

Каланча І.Г. Використання висновку експерта, що має електронну форму як доказу в кримінальному процесі України. *Актуальні проблеми національного законодавства: збірник матеріалів Міжнародної науково-практичної конференції*, м. Кропивницький, 17 квітня 2025 року. Частина 1. Кропивницький, 2025. С. 154-156. URL: https://www.researchgate.net/publication/392901845_Kalanca_IG_Vikoristannya_v_isnovku_eksperta_so_mae_elektronnu_formu_ak_dokazu_v_kriminalnomu_procesi_Ukraini_Aktualni_problemi_nacionalnogo_zakonodavstva_zbirnik_materialiv_Miznarodnoi_naukovo-prakticno

На основі проведеного аналізу комісія дійшла висновку, що публікації Каланчі І.Г. містять науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання в освітньому процесі Київського столичного університету імені Бориса Грінченка при викладанні навчальних курсів «Кримінальне процесуальне право», «Судові навички», «Складання процесуальних документів», під час підготовки навчально-методичних та дидактичних матеріалів, а також рекомендувати їх до вивчення під час самостійної роботи здобувачів вищої освіти.

Члени комісії:

Завідувач кафедри публічного права
факультету права та міжнародних відносин
Київського столичного університету
імені Бориса Грінченка,
доктор юридичних наук, професор,
заслужений діяч науки і техніки України



Ганна ЦИМБАЛ

Професор кафедри публічного права
факультету права та міжнародних відносин
Київського столичного університету
імені Бориса Грінченка,
доктор юридичних наук, доцент



Володимир ЗАВИДНЯК

Доцент кафедри публічного права
факультету права та міжнародних відносин
Київського столичного університету
імені Бориса Грінченка,
доктор філософії в галузі права



Андрій ЛІСЦЬКИЙ

ЗАТВЕРДЖУЮ

Проректор з навчально-методичної
роботи ПВНЗ «Європейський
університет», доктор філософський
наук, професор

Ягодзінський С. М.

_____ 2025 року

**АКТ впровадження результатів дисертаційного дослідження Каланчі
Інги Георгіївни на тему: «Докази електронної форми в кримінальному
процесі України: теорія і практика» освітній процес.**

« 20 » жовтня 2025 року

м. Київ

Комісія у складі:

завідувача кафедри права ПВНЗ «Європейський університет»
доктора юридичних наук, професора, заслуженого юриста України
Цимбала Петра Васильовича,

професора кафедри права ПВНЗ «Європейський університет»
кандидата юридичних наук, доцента Тимошенко Ольги Анатоліївни,

директора Центру забезпечення якості освіти ПВНЗ «Європейський
університет» кандидата юридичних наук, доцента Кузьменко Олени
Валеріївни,

розглянула й узагальнила результати дисертаційного дослідження
здобувачки кафедри кримінального процесу Національної академії внутрішніх
справ Каланчі Інги Георгіївни на тему: «Докази електронної форми у
кримінальному процесі України: теорія та практика», поданого на здобуття
наукового ступеня доктора юридичних наук зі спеціальності 12.00.09 -
кримінальний процес та криміналістика; судова експертиза; оперативно-
розшукова діяльність. На основі проведеного аналізу комісія зробила
висновок, що надані наукові праці містять низку обґрунтованих теоретичних
положень і пропозицій, спрямованих на теоретичне дослідження доказів
електронної форми у кримінальному процесі України.

Проаналізовано основні результати дослідження Каланчі І.Г., зокрема
наукові праці, в яких опубліковані положення дисертаційного дослідження:

Каланча І.Г. Електронний сегмент в кримінальному процесуальному
законі Азербайджану. *Науковий вісник Ужгородського національного
університету. Серія «Право». №59. 2019. С. 117-121.*
DOI: <https://doi.org/10.32782/2307-3322.59-2.26>

Каланча І.Г. Електронний сегмент кримінального процесу Естонії. *Порівняльно-аналітичне право*, №3, 2019. С. 212-216. URL: https://pap-journal.in.ua/wp-content/uploads/2021/07/3_2019.pdf

Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. № 146, 2019. С. 179-191. DOI: <https://doi.org/10.21564/2414-990x.146.171218>

Каланча І.Г. Електронний сегмент в кримінальному процесі Грузії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №4, 2019. С. 161-166. DOI: <https://doi.org/10.31733/2078-3566-2019-4-161-166>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законодавстві Молдови. *Jurnalul Juridic National: teorie si practica*. №1 (41). 2020. С. 132-137. URL: <http://www.jurnaluljuridic.in.ua/archive/2020/1/30.pdf>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Туркменістану. *Актуальні проблеми вітчизняної юриспруденції*. № 1. 2020. С. 91-95. DOI: <https://doi.org/10.15421/392021> URL: http://apnl.dnu.in.ua/1_2020/23.pdf

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Вірменії. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. №1. 2020. С. 205-210. DOI: <https://doi.org/10.31733/2078-3566-2020-1-205-210>

Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Латвії. *Криміналістика і судова експертиза : міжвідомчий науково-методичний збірник*. Вип. 65, 2020. С. 90-100. DOI: <https://doi.org/10.33994/kndise.2020.65.09>

Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал*, №8, 2021. С. 336-339. DOI: <https://doi.org/10.32782/2524-0374/2021-8/77>

Patreliuk, D., Svoboda, I., Kalancha, I., Filashkin, V., Kachmar, B. Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations. *Pakistan Journal of Life and Social Sciences*, 2024, 22(2), pp. 4811–4820. DOI: <https://doi.org/10.57239/PJLSS-2024-22.2.00356>

Каланча І.Г., Орлеан А.М. Адаптація системи кримінальної юстиції до цифровізації світу : роль навчального компоненту. *Наукові перспективи*, №11 (53), 2024. С. 937-944. DOI: [https://doi.org/10.52058/2708-7530-2024-11\(53\)-937-944](https://doi.org/10.52058/2708-7530-2024-11(53)-937-944)

Каланча І.Г., Юрчишин Ю.В. Забезпечення безпеки прокурора під час роботи з електронним сегментом кримінального провадження в Україні. *Вчені записки Таврійського національного університету імені В. І. Вернадського*.

Серія: Юридичні науки. Том 35 (74) № 6, 2024. С. 108-115. DOI: <https://doi.org/10.32782/TNU-2707-0581/2024.6/19>

Каланча І.Г. Алгоритм електронного кримінального провадження. *Law. State. Technology*, 2024. Вип. 4, С. 69-74. DOI: <https://doi.org/10.32782/LST/2024-4-13>

Каланча І.Г. Практика роботи з доказами, що мають електронну форму в кримінальному процесі України : соціологічне дослідження. *Успіхи і досягнення у науці*. №1(11). 2025. С. 76-93. DOI: [https://doi.org/10.52058/3041-1254-2025-1\(11\)-76-93](https://doi.org/10.52058/3041-1254-2025-1(11)-76-93)

Каланча І.Г., Стемковський Д.Б. Використання доказів, що мають електронну форму в кримінальному процесі України: судова практика. *Аналітично-порівняльне правознавство*. 2025. №2. С. 1001-1008. DOI: <https://doi.org/10.24144/2788-6018.2025.02.148> <https://app-journal.in.ua/wp-content/uploads/2025/04/150.pdf>

Каланча І.Г. Електронний висновок експерта як доказ у кримінальному процесі України: практика, перспективи та ризики. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. №2. С. 84-92. DOI: <https://doi.org/10.32782/2311-8040/2025-2-12> URL: <http://journals.lvduvs.lviv.ua/index.php/law/article/view/981/953>

Каланча І.Г. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світлі концепції chain of custody. *Věda a perspektivy*. № 8(51) (2025). С. 206-230. URL: https://www.researchgate.net/publication/394998880_Kalanca_IG_Dokazi_so_maut_elektronnu_formu_v_kriminalnomu_procesi_Ukraini_identifikacia_ta_cilisnist_u_svitli_koncepcii_chain_of_custody_Veda_a_perspektivy_No_851_2025_C_206-230

Kozii, V.; Kalancha, I.; Vlasova, H.; Orlean, A. Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies. *IDP. Internet, Law an Politics Journal*, 2025, no. 42. pp. 1-13. DOI: <http://dx.doi.org/10.7238/idp.v0i42.429924> URL: <https://raco.cat/index.php/IDP/article/view/429924/526486>

Каланча І.Г. Процесуальна природа доказів, що мають електронну форму в кримінальному процесі України: документ та речовий доказ. *Міжнародний науковий журнал "Інтернаука". Серія: "Юридичні науки"*. № 7. 2025. С. 85-92. DOI <https://doi.org/10.25313/2520-2308-2025-7-11208> URL: <https://www.inter-nauka.com/uploads/public/17557614844770.pdf>

Каланча І.Г. Організаційні аспекти роботи з доказами, що мають електронну форму в кримінальному процесі України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. Вип. 90, Ч. 4. 2025. С. 258-266. DOI <https://doi.org/10.24144/2307-3322.2025.90.4.36>

Каланча І.Г. Єдине електронне інформаційне поле органів кримінальної юстиції. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : мат. міжн. наук.-практ. конф. (м. Київ, 5.11.2019 р.). К., 2019. С. 209-213. URL: https://www.researchgate.net/publication/393743748_Kalanca_IG_Edine_elektronne_informacijne_pole_organiv_kriminalnoi_usticii_Aktualni_pitanna_sudovoi_eksptologiji_kriminalistiki_ta_kriminalnogo_procesu_mat_mizn_nauk-prakt_konf_m_Kiiv_5112019_r_K_2019

Каланча І.Г. Шляхи формування сучасних практичних компетентностей у випускників правничих шкіл України. *Інноваційні рішення в сучасній науці, освіті та практиці*: Матеріали I Міжнародної науково-практичної інтернет-конференції (наукове видання), 17-18 листопада 2020 р.: у 2 ч. Київ: НТУ, 2020. Ч.2. С. 209-212. URL: <http://vstup.ntu.edu.ua/conf-innov-part-2.pdf>

Гаркуша А.М., Каланча І.Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи*: матеріали круглого столу (м. Львів, 11 червня 2021 р.). Львів: Львівський державний університет внутрішніх справ., 2021. С. 159-165. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/11_06_2021.pdf

Каланча І.Г. Підходи до класифікації електронних носіїв інформації та інформаційних систем для завдань кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали V Міжнар. наук.-практ. конф. (29 жовтня 2021р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2021. С. 211-213. URL: <https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk-29.10.21.pdf>

Гаркуша А.М., Каланча І.Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. *Наукові читання пам'яті Ганса Гросса*: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівецький національний університет імені Юрія Федьковича. Чернівці : Технодрук, С. 72-75. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/11383/Forensic_Epi_stemology_Czernowitz_2021_.pdf?sequence=1&isAllowed=y

Каланча І.Г. Окремі аспекти діяльності прокурора щодо гарантування цілісності доказів, що мають електронну форму під час досудового розслідування кримінального провадження. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VI Міжнар. наук.-практ. конф. (21 жовтня 2022р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2022. С. 327-332. URL: https://ccu.gov.ua/sites/default/files/suchasni_vyklyky_ta_aktualni_problemy_sudovoyi_reformy_v_ukrayini_2022.pdf

Каланча І.Г. Способи ідентифікації комп'ютерних даних як доказу в кримінальному провадженні. *III Наукові читання пам'яті Ганса Гросса* : збірник тез міжнародної науково-практичної конференції (м. Чернівці, 08 грудня 2023 р.). Чернівці: Чернівець. нац. У-нт ім. Ю.Федьковича, 2023. С. 71-75. URL: <https://www.ndekc.cv.ua/wp-content/uploads/2024/03/III-Naukovi-chytannya-pam-yati-Gansa-Grossa.pdf>

Каланча І.Г. Стратегії фіксації доказів, що мають електронну форму для застосування в кримінальному провадженні. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VII Міжнар. наук.-практ. конф. (27 жовтня 2023р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2023. С. 253-258. URL: https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk_conf_27..pdf

Каланча І.Г. Кіберпростір як територія проведення досудового розслідування. *Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини*: зб. наук. праць за матер. Круглого столу, Київ, 7 грудня 2023 р. / редкол.: А.Ю. Нашинець-Наумова, Г.П. Власова, С.В. Бобровник, Т.О. Дідич, Н.А. Сергієнко, А.П. Чернега. – К. : Київ. стол. ун-т ім. Б. Грінченка, 2024. С. 115-119. URL: <https://kubg.edu.ua/struktura/pidrozdiili/yurydychna-klinika-astreya/zakhody/8438-ikh-kruhlyi-stil-prava-liudyny-v-umovakh-voiennoho-stanu-v-ukraini.html>

Каланча І.Г. Цифрова складова кримінального процесу України в науці та практиці: структурно-функціональний аналіз. *Сучасні виклики та актуальні проблеми судової реформи в Україні*: Матеріали VIII Міжнар. наук.-практ. конф. (31 жовтня 2024р., Чернівці)/ редкол.: О.В. Щербанюк та ін. - Чернівці: 2024. С. 229-233. URL: https://www.researchgate.net/publication/390005117_Kalanca_IG_Cifrova_sklado_va_kriminalnogo_procesu_Ukraini_v_nauci_ta_praktici_strukturno-funkcionalnij_analiz_Sucasni_vikliki_ta_aktualni_problemi_sudovoi_reformi_v_Ukraini_Materiali_VIII_Miznar_nauk-p

Каланча І.Г. Матеріальна форма існування як властивість доказу в кримінальному процесі України: практика правозастосування. *Права людини в умовах воєнного стану в Україні: X круглий стіл до Всеукраїнського тижня права (10 грудня 2024 року). Права людини в умовах воєнного стану в Україні: до тижня права і Загальної декларації прав людини* : зб. наук. праць за матер. круглого столу, Київ, 10 грудня 2024 р. / редкол.: А.Ю. Нашинець-Наумова, Г.П. Цимбал, С.В. Бобровник, Т.О. Дідич, О.І. Чаплук, А.П. Чернега. — Київ : Київ. столич. ун-т ім. Б. Грінченка, 2025. С. 63-67. URL: https://www.researchgate.net/publication/396154856_Kalanca_IG_Materialna_forma_isnuvanna_ak_vlastivist_dokazu_v_kriminalnomu_procesi_Ukraini_praktika_pravozastosuvannya_Prava_ludini_v_umovah_voennogo_stanu_v_Ukraini_X_kruglii_stil_do_Vseukrainskogo_tiz

Каланча І. Термінологічне розмежування понять «електронний доказ», «цифровий доказ» і «доказ, що має електронну форму» в кримінальному

процесі України. *Пріоритетні шляхи розвитку науки і освіти*: матеріали XV Міжнародної науково-практичної конференції м. Львів, 9-10 травня 2025 року. – Львів : Львівський науковий форум, 2025. С. 195-197. URL: <http://www.lviv-forum.inf.ua/save/2025/9-10.05/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA.pdf>

Власова Г.П., Каланча І.Г. Захисник як суб'єкт роботи з електронними доказами в кримінальному провадженні. *Актуальні питання реформування правової системи : зб. матеріалів XXII Міжнар. наук.-практ. конф., Луцьк, 13-15 червня 2025 р. / Уклад. Джурак Л. М. – Луцьк : Вежа-Друк, 2025. С. 113-115.* URL: https://www.law.vnu.edu.ua/_files/ugd/65dd18_5ab2de833d004115b0483aa2420d7cc0.pdf

Каланча І.Г. Результати OSINT як джерело доказів у кримінальному процесі України. *Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій*: Матеріали Всеукр. наук.-практ. конф. (м. Чернівці, 20 грудня 2024 р.) / відп. ред. К.А. Возняковська. ТОМ 1, Чернівці, 2024. С. 43-49. URL: https://www.researchgate.net/publication/389647938_Kalanca_IG_Rezultati_OSINT_ak_dzerelo_dokaziv_u_kriminalnomu_procesi_Ukraini_Innovacii_vikliki_ta_novi_gorizonti_pravovogo_reguluvanna_u_svitli_sucasnih_socialno-ekonomichnih_ta_politicnih_transformaci

Каланча І.Г. Використання висновку експерта, що має електронну форму як доказу в кримінальному процесі України. *Актуальні проблеми національного законодавства*: збірник матеріалів Міжнародної науково-практичної конференції, м. Кропивницький, 17 квітня 2025 року. Частина 1. Кропивницький, 2025. С. 154-156. URL: https://www.researchgate.net/publication/392901845_Kalanca_IG_Vikoristanna_v_isnovku_eksperta_so_mae_elektronnu_formu_ak_dokazu_v_kriminalnomu_procesi_Ukraini_Aktualni_problemi_nacionalnogo_zakonodavstva_zbirk_materialiv_Miznarodnoi_naukovo-prakticno

На основі проведеного аналізу комісія дійшла висновку, що публікації Каланчі І.Г. містять науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання в освітньому процесі ПВНЗ «Європейський університет» при викладанні навчальних курсів «Кримінальне процесуальне право», «Судові навички», «Складання процесуальних документів», під час підготовки навчально-методичних та дидактичних матеріалів, а також рекомендувати їх до вивчення під час самостійної роботи здобувачів вищої освіти.

Члени комісії:

Завідувач кафедри права
ПВНЗ «Європейський університет»
доктор юридичних наук, професор,
заслужений юрист України



Петро ЦИМБАЛ

Професор кафедри права
ПВНЗ «Європейський університет»
кандидат юридичних наук,
доцент



Ольга ТИМОШЕНКО

Директор Центру забезпечення якості освіти
ПВНЗ «Європейський університет»
кандидат юридичних наук, доцент



Олена КУЗЬМЕНКО



КОМІТЕТ ВЕРХОВНОЇ РАДИ УКРАЇНИ з питань правоохоронної діяльності

вул. М. Грушевського, 5, м. Київ, 01008, www.rada.gov.ua

**Київський столичний університет
імені Бориса Грінченка
Каланчі І.Г.**

Шановна Інго Георгіївно!

У Комітеті Верховної Ради України з питань правоохоронної діяльності розглянуто зміни до Кримінального процесуального кодексу України, підготовлені Вами у межах здійснення дисертаційного дослідження на тему: «Докази електронної форми у кримінальному процесі України: теорія та практика».

За результатами розгляду повідомляємо, що розроблені в межах дисертаційного дослідження пропозиції, які оформлені у вигляді проекту Закону України «Про внесення змін та доповнень до Кримінального процесуального кодексу України щодо врегулювання роботи з доказами електронної форми під час кримінального провадження», надані для ознайомлення народним депутатам України – членам Комітету Верховної Ради України з питань правоохоронної.

**З повагою
Голова Комітету**

С. Іонушас



САС ВЕРХОВНОЇ РАДИ УКРАЇНИ
Підписувач: Іонушас Сергій Костянтинович
Сертифікат: 3F4A9288358DC0039400000000512F003B628C00
Дійсний до: 12.12.2026 0:00:00

Апарат Верховної Ради України
04-27/11-2025/261827 від 13.11.2025
2055007

Додаток У

ЗАТВЕРДЖУЮ
 Начальник
 Департаменту кіберполіції
 Національної поліції України
 генерал-поліції третього рангу


 Юрій ВИХОДЕЦЬ
 2025 року

АКТ № 5

Про впровадження в практичну діяльність
 Департаменту кіберполіції Національної
 поліції України результатів дисертаційного
 дослідження Каланчі Інги Георгіївни на тему:
 «Докази електронної форми в кримінальному
 процесі України: теорія і практика»

Комісія у складі:

голови: першого заступника начальника Департаменту
 кіберполіції Національної поліції України
 полковника поліції Андрія ШАРОНОВА

членів комісії: начальника 3-го управління (інформаційних
 технологій та програмування) Департаменту
 кіберполіції Національної поліції України кандидата
 юридичних наук, полковника поліції Станіслава
 САМОЙЛОВА

начальника 5-го відділу (інформаційних технологій
 та програмування в південному регіоні) (м. Одеса) 3-
 го управління (інформаційних технологій та
 програмування) Департаменту кіберполіції
 Національної поліції України кандидата юридичних
 наук, доцента, підполковника поліції Карена
 ІСМАЙЛОВА

відповідно до доручення Міністерства внутрішніх справ України від
 11.11.2022 № 151/48 «Про заходи з реалізації наукової та науково-технічної
 політики Міністерства внутрішніх справ України», склала цей акт про розгляд
 результатів дисертаційного дослідження здобувачки кафедри кримінального
 процесу Національної академії внутрішніх справ Каланчі Інги Георгіївни на
 тему: «Докази електронної форми у кримінальному процесі України: теорія та

практика», поданого на здобуття наукового ступеня доктора юридичних наук зі спеціальності 12.00.09 - кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. На основі проведеного аналізу комісія зробила висновок, що надані наукові праці Каланчі І.Г. містять низку обґрунтованих наукових положень і пропозицій щодо доказів електронної форми у кримінальному процесі України.

Прованалізовано результати дисертаційного дослідження Каланчі І.Г., що відображені в наступних наукових публікаціях:

- Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Азербайджану. Науковий вісник Ужгородського національного університету. Серія «Право». №59. 2019. С. 117-121. DOI: <https://doi.org/10.32782/2307-3322.59-2.26>

- Каланча І.Г. Електронний сегмент кримінального процесу Естонії. Порівняльно-аналітичне право, №3, 2019. С. 212-216. URL: https://pap-journal.in.ua/wp-content/uploads/2021/07/3_2019.pdf

- Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України. Проблеми законності. № 146, 2019. С. 179-191. DOI: <https://doi.org/10.21564/2414-990x.146.171218>

- Каланча І.Г. Електронний сегмент в кримінальному процесі Грузії. Науковий вісник Дніпропетровського державного університету внутрішніх справ. №4, 2019. С. 161-166. DOI: <https://doi.org/10.31733/2078-3566-2019-4-161-166>

- Каланча І.Г. Електронний сегмент в кримінальному процесуальному законодавстві Молдови. Jurnalul Juridic National: teorie si practica. №1 (41), 2020. С. 132-137. URL: <http://www.jurnaluljuridic.in.ua/archive/2020/1/30.pdf>

- Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Туркменістану. Актуальні проблеми вітчизняної юриспруденції. № 1. 2020. С. 91-95. DOI: <https://doi.org/10.15421/392021> URL: http://apnl.dnu.in.ua/1_2020/23.pdf

- Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Вірменії. Науковий вісник Дніпропетровського державного університету внутрішніх справ. №1. 2020. С. 205-210. DOI: <https://doi.org/10.31733/2078-3566-2020-1-205-210>

- Каланча І.Г. Електронний сегмент в кримінальному процесуальному законі Латвії. Криміналістика і судова експертиза : міжвідомчий науково-методичний збірник. Вип. 65, 2020. С. 90-100. DOI: <https://doi.org/10.33994/kndise.2020.65.09>

- Каланча І.Г., Гаркуша А.М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. Юридичний науковий електронний журнал, №8, 2021. С. 336-339. DOI: <https://doi.org/10.32782/2524-0374/2021-8/77>

- Patreliuk, D., Svoboda, I., Kalancha, I., Filashkin, V., Kachmar, B. Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations. Pakistan Journal of Life and Social Sciences, 2024, 22(2), pp. 4811-4820. DOI: <https://doi.org/10.57239/PJLSS-2024-22.2.00356>

• Каланча І.Г., Орлеан А.М. Адаптація системи кримінальної юстиції до цифровізації світу : роль навчального компоненту. Наукові перспективи, №11 (53), 2024. С. 937-944. DOI: [https://doi.org/10.52058/2708-7530-2024-11\(53\)-937-944](https://doi.org/10.52058/2708-7530-2024-11(53)-937-944)

• Каланча І.Г., Юрчишин Ю.В. Забезпечення безпеки прокурора під час роботи з електронним сегментом кримінального провадження в Україні. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки. Том 35 (74) № 6, 2024. С. 108-115. DOI: <https://doi.org/10.32782/TNU-2707-0581/2024.6/19>

• Каланча І.Г. Алгоритм електронного кримінального провадження. Law. State. Technology, 2024. Вип. 4, С. 69-74. DOI: <https://doi.org/10.32782/LST/2024-4-13>

• Каланча І.Г. Практика роботи з доказами, що мають електронну форму в кримінальному процесі України : соціологічне дослідження. Успіхи і досягнення у науці. №1(11). 2025. С. 76-93. DOI: [https://doi.org/10.52058/3041-1254-2025-1\(11\)-76-93](https://doi.org/10.52058/3041-1254-2025-1(11)-76-93)

• Каланча І.Г., Стемковський Д.Б. Використання доказів, що мають електронну форму в кримінальному процесі України: судова практика. Аналітично-порівняльне правознавство. 2025. №2. С. 1001-1008. DOI: <https://doi.org/10.24144/2788-6018.2025.02.148> <https://app-journal.in.ua/wp-content/uploads/2025/04/150.pdf>

• Каланча І.Г. Електронний висновок експерта як доказ у кримінальному процесі України: практика, перспективи та ризики. Науковий вісник Львівського державного університету внутрішніх справ (серія юридична). 2025. №2. С. 84-92. DOI: <https://doi.org/10.32782/2311-8040/2025-2-12> URL: <http://journals.lvduvs.lviv.ua/index.php/law/article/view/981/953>

• Каланча І.Г. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світлі концепції chain of custody. Věda a perspektivy. № 8(51) (2025). С. 206-230. URL: https://www.researchgate.net/publication/394998880_Kalanca_IG_Dokazi_so_ma_ut_elektronnu_formu_v_kriminalnomu_procesi_Ukraini_identifikacia_ta_cilisnist_u_svitli_koncepcii_chain_of_custody_Veda_a_perspektivy_No_851_2025_C_206-230

• Kozii, V.; Kalancha, I.; Vlasova, H.; Orlean, A. Peculiarities of recording electronic evidence in criminal proceedings regarding crimes committed in Ukraine using cryptocurrencies. IDP. Internet, Law an Politics Journal, 2025, no. 42. pp. 1-13. DOI: <http://dx.doi.org/10.7238/idp.v0i42.429924> URL: <https://raco.cat/index.php/IDP/article/view/429924/526486>

• Каланча І.Г. Процесуальна природа доказів, що мають електронну форму в кримінальному процесі України: документ та речовий доказ. Міжнародний науковий журнал "Інтернаука". Серія: "Юридичні науки". № 7, 2025. С. 85-92. DOI: <https://doi.org/10.25313/2520-2308-2025-7-11208> URL: <https://www.inter-nauka.com/uploads/public/17557614844770.pdf>

• Каланча І.Г. Організаційні аспекти роботи з доказами, що мають електронну форму в кримінальному процесі України. Науковий вісник

Ужгородського національного університету. Серія «Право». Вип. 90, Ч. 4. 2025. С. 258-266. DOI <https://doi.org/10.24144/2307-3322.2025.90.4.36>

• Каланча І.Г. Єдине електронне інформаційне поле органів кримінальної юстиції. Актуальні питання судової експертології, криміналістики та кримінального процесу: мат. міжн. наук.-практ. конф. (м. Київ, 5.11.2019 р.). К., 2019. С. 209-213. URL: https://www.researchgate.net/publication/393743748_Kalanca_IG_Edine_elektronne_informacijne_pole_organiv_kriminalnoi_usticii_Aktualni_pitanna_sudovoi_ekspernologii_kriminalistiki_ta_kriminalnogo_procesu_mat_mizn_nauk-prakt_konf_m_Kiiv_5112019_r_K_2019

• Каланча І.Г. Шляхи формування сучасних практичних компетентностей у випускників правничих шкіл України. Інноваційні рішення в сучасній науці, освіті та практиці: Матеріали I Міжнародної науково-практичної інтернет-конференції (наукове видання), 17-18 листопада 2020 р.: у 2 ч. Київ: НТУ, 2020. Ч.2. С. 209-212. URL: <http://vstup.ntu.edu.ua/conf-innov-part-2.pdf>

• Гаркуша А.М., Каланча І.Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. Кримінальна юстиція в Україні: реалії та перспективи: матеріали круглого столу (м. Львів, 11 червня 2021 р.). Львів: Львівський державний університет внутрішніх справ, 2021. С. 159-165. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/11_06_2021.pdf

• Каланча І.Г. Підходи до класифікації електронних носіїв інформації та інформаційних систем для завдань кримінального провадження. Сучасні виклики та актуальні проблеми судової реформи в Україні: Матеріали V Міжнар. наук.-практ. конф. (29 жовтня 2021р., Чернівці) редкол.: О.В. Щербанюк та ін. Чернівці: 2021. С. 211-213. URL: <https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk-29.10.21.pdf>

• Гаркуша А.М., Каланча І.Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. Наукові читання пам'яті Ганса Гросса: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівський національний університет імені Юрія Федьковича. Чернівці: Технодрук, С. 72-75. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/11383/Forensic_Epistemology_Czernowitz_2021_.pdf?sequence=1&isAllowed=y

• Каланча І.Г. Окремі аспекти діяльності прокурора щодо гарантування цілісності доказів, що мають електронну форму під час досудового розслідування кримінального провадження. Сучасні виклики та актуальні проблеми судової реформи в Україні: Матеріали VI Міжнар. наук.-практ. конф. (21 жовтня 2022р., Чернівці) редкол.: О.В. Щербанюк та ін. Чернівці: 2022. С. 327-332. URL: https://ccu.gov.ua/sites/default/files/suchasni_vyklyky_ta_aktualni_problemy_sudovoyi_reformy_v_ukrayini_2022.pdf

• Каланча І.Г. Способи ідентифікації комп'ютерних даних як доказу в кримінальному провадженні. III Наукові читання пам'яті Ганса Гросса: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 08

грудня 2023 р.), Чернівці: Чернівець. нац. У-нт. ім. Ю.Федьковича, 2023. С. 71-75. URL: <https://www.ndekc.cv.ua/wp-content/uploads/2024/03/III-Naukovi-chytannya-pam-yati-Gansa-Grossa.pdf>

• Каланча І.Г. Стратегії фіксації доказів, що мають електронну форму для застосування в кримінальному провадженні. Сучасні виклики та актуальні проблеми судової реформи в Україні: Матеріали VII Міжнар. наук.-практ. конф. (27 жовтня 2023р., Чернівці)/ редкол.: О.В. Щербанюк та ін. Чернівці: 2023. С. 253-258. URL:

https://law.chnu.edu.ua/wp-content/uploads/docs/zbirnyk_conf_27..pdf

• Каланча І.Г. Кіберпростір як територія проведення досудового розслідування. Права людини в умовах воєнного стану в Україні: до тижня права і 75-річчя Загальної декларації прав людини: зб. наук. праць за матер. Круглого столу, Київ, 7 грудня 2023 р. / редкол.: А.Ю. Нашинець-Наумова, Г.П. Власова, С.В. Бобровник, Т.О. Дідич, Н.А. Сергієнко, А.П. Чернега. – К.: Київ. стол. ун-т ім. Б. Грінченка, 2024. С. 115-119. URL: <https://kubg.edu.ua/struktura/pidroz dili/yurydychna-klinika-astreya/zakhody/8438-ikh-kruhlyi-stil-prava-liudyny-v-umovakh-voiennoho-stanu-v-ukraini.html>

• Каланча І.Г. Цифрова складова кримінального процесу України в науці та практиці: структурно-функціональний аналіз. Сучасні виклики та актуальні проблеми судової реформи в Україні: Матеріали VIII Міжнар. наук.-практ. конф. (31 жовтня 2024р., Чернівці)/ редкол.: О.В. Щербанюк та ін. - Чернівці: 2024. С. 229-233. URL: https://www.researchgate.net/publication/390005117_Kalanca_IG_Cifrova_sklado_va_kriminalnogo_procesu_Ukraini_v_nauci_ta_praktici_strukturno-funkcionalnij_analiz_Sucasni_vikliki_ta_aktualni_problemi_sudovoi_reformi_v_Ukraini_Materiali_VIII_Miznar_nauk-p

• Каланча І.Г. Результати OSINT як джерело доказів у кримінальному процесі України. Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій: Матеріали Всеукр. наук.-практ. конф. (м. Чернівці, 20 грудня 2024 р.) / відп. ред. К.А. Возняковська. ТОМ 1, Чернівці, 2024. С. 43-49. URL: https://www.researchgate.net/publication/389647938_Kalanca_IG_Rezultati_OSINT_ak_dzerelo_dokaziv_u_kriminalnomu_procesi_Ukraini_Innovacii_vikliki_ta_novi_gorizonti_pravovogo_reguluvanna_u_svitli_sucasnih_socialno-ekonomichnih_ta_politicnih_transformaci

• Каланча І.Г. Використання висновку експерта, що має електронну форму як доказу в кримінальному процесі України. Актуальні проблеми національного законодавства: збірник матеріалів Міжнародної науково-практичної конференції, м. Кропивницький, 17 квітня 2025 року. Частина 1. Кропивницький, 2025. С. 154-156. URL: https://www.researchgate.net/publication/392901845_Kalanca_IG_Vikoristanna_v_isnovku_eksperta_so_mae_elektronnu_formu_ak_dokazu_v_kriminalnomu_procesi_Ukraini_Aktualni_problemi_nacionalnogo_zakonodavstva_zbirnik_materialiv_Miznarodnoi_naukovo-prakticno

За результатами проведеного аналізу комісія дійшла висновку, що основні положення дисертаційного дослідження Каланчі І.Г. мають практичну

цінність та можуть бути використані в практичній діяльності Департаменту кіберполіції Національної поліції України, зокрема: при підготовці методичних рекомендацій щодо особливостей проведення слідчих (розшукових) дій, спрямованих на виявлення та фіксацію доказів електронної форми; у роботу підрозділів кіберполіції з документування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; під час розроблення внутрішніх інструкцій з організації роботи; у процесі навчання та підвищення кваліфікації співробітників Департаменту кіберполіції Національної поліції України.

Голова комісії

Андрій ШАРОНОВ

Члени комісії:

Станіслав САМОЙЛОВ

Карен ІСМАЙЛОВ

Додаток Ф



Прокуратура України
ОФІС ГЕНЕРАЛЬНОГО ПРОКУРОРА

вул. Різницька, 13/15, м. Київ, 01011 факс: (044) 280-26-03 e-mail: office@gp.gov.ua, web: www.gp.gov.ua
Код ЄДРПОУ 00034051

21.11.2015 №18/4-36908-15

На № _____ від _____

**Київський столичний університет імені
Бориса Грінченка**
Доценту кафедри публічного права
факультету права та міжнародних
відносин, к.ю.н.
Іллі КАЛАНЧІ
i.kalancha@kubg.edu.ua

Забезпечення належного розслідування у кримінальних провадженнях за фактами вчинення серйозних порушень міжнародного гуманітарного права є пріоритетом роботи органів прокуратури та органів правопорядку в умовах збройного конфлікту. Важливою складовою результативного досудового розслідування та судового розгляду злочинів відповідної категорії є ефективна робота з доказами електронної форми.

Департамент протидії злочинам, вчиненим в умовах збройного конфлікту, Офісу Генерального прокурора висловлює вдячність факультету права та міжнародних відносин Київського столичного університету імені Бориса Грінченка за експертну підтримку в опрацюванні актуальних питань кримінального процесуального права в частині доказів електронної форми.

Зокрема, Департаментом отримано та використовуються у практичній діяльності результати дисертації «Докази електронної форми у кримінальному процесі України: теорія та практика», підготовлені доцентом кафедри публічного права факультету права та міжнародних відносин Київського столичного університету імені Бориса Грінченка, к.ю.н. Інною Каланчею.

Представлені І. Каланчею матеріали мають практичну цінність для правильного застосування норм кримінального процесуального права, підготовки процесуальних документів та обґрунтування рішень у кримінальному провадженні.

Підсумовуючи, ми ще раз дякуємо за існуючу співпрацю та висловлюємо надію на її розширення.

Начальник
Департаменту протидії злочинам,
вчиненим в умовах збройного конфлікту,
Офісу Генерального прокурора

Юрій РУДЬ