

6. Matulienė, S., Shevchuk, V., & Baltrūnienė, J. Artificial Intelligence in Law Enforcement and Justice Bodies: Domestic and European Experience. *Theory and Practice of Forensic Science and Criminalistics*, 2023, 29(4), 12-46.

7. Shevchuk, V., Zhuravel, V., Yevdokimenko, S., Yevdokimenko, S., Myshkov, Y. (2025). Forensic Examination and Criminalistics in Investigating War Crimes: European and Ukrainian Experiences. *Jurnal Media Hukum*, 32(1), 59-77.

8. Шевчук В. М. Криміналістична техніка: сучасні проблеми та перспективи розвитку. *Dynamics of the development of world science* : abstr. of IX intern. and practical conf. (May 13–15, 2020). Vancouver, 2020. P. 1068–1078.

9. Шевчук В. М. Роль криміналістичної поліграфології у кримінальному провадженні та системі забезпечення безпеки і оборони України. Сучасний досвід використання поліграфа у сфері національної безпеки і оборони України в умовах воєнних загроз: зб. матеріалів панел. дискусії : IX Харків. міжнар. юрид. форум, м. Харків, 26 верес. 2025 р.; Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. криміналістики [та ін.]. Харків : Право, 2025. С. 138–147.

10. Shevchuk V., Morozova T., Chorny H., Nehrebetskyi V., Slobodeniuk I. Artificial Intelligence in Criminal Proceedings: Criminalistic and Criminal Procedural Problems. *International Annals of Criminology*, 2025. P. 1–19. DOI: <https://doi.org/10.1017/cri.2025.10090>

Шепітько Валерій Юрійович,

професор кафедри криміналістики
Національного юридичного університету
імені Ярослава Мудрого, доктор
юридичних наук, професор, академік
Національної академії правових наук
України

ЦИФРОВІ ДОКАЗИ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ ТА ПРОБЛЕМА СТАНДАРТИЗАЦІЇ РОЗСЛІДУВАННЯ

Невід’ємною складовою будь-якої процесуальної галузі права є інститут доказів та доказування. Розслідування злочинів або судовий розгляд – це завжди «боротьба за інформацію».

Розслідування має точно встановлювати обставини кримінального провадження, адекватно відображати подію кримінального правопорушення, ситуації, осіб, винних у його вчиненні [1, с. 16].

В юридичній доктрині існують різні підходи до розуміння доказів. Докази розглядають як «факти реальної дійсності», «будь-які фактичні дані, що мають значення для кримінального провадження», «відповідний носій (джерело) відомостей про них», «процесуальну процедуру та форму (спосіб) її закріплення в матеріалах кримінального провадження». Відповідно до ст. 84 КПК України доказами в кримінальному провадженні є фактичні дані, отримані в передбаченому порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

У криміналістичному сенсі лексичні словосполучення «фактичні дані (обставини)», «відомості, що містяться у показаннях», «відомості, отримані під час дослідження речей, документів, матеріальних слідів злочину» тощо, які вживаються у процесуальному законі не вирішують проблему щодо формування доказової інформації (доказів). Вважаємо, що «відомості», «фактичні обставини» або «дані» мають бути перевірені під час судового розгляду, а також на цій стадії кримінального провадження підтверджено їх статус як доказів.

Окремої уваги заслуговують так звані цифрові докази (цифрова інформація) – інформація, яка створена за допомогою високих інформаційних технологій. Поряд із терміном «цифрові докази» у різних джерелах використовуються й інші, наприклад: «електронні докази» [2], «електронні сліди», «цифрові джерела інформації», «електронні документи», комп'ютерні дані тощо. При цьому, «навколо визначення, змісту, а також процесуального порядку отримання, оцінювання й використання інформації, що зберігається на електронних носіях у фаховому середовищі точаться запеклі наукові дискусії» [2, с. 228].

У наукових джерелах зарубіжних країн широкого застосування набув термін «digital evidences» (цифрові докази), під якими розуміють будь-які збережені дані або дані, що передаються з використанням комп'ютерної чи іншої техніки [3, с. 257]. Цифрові докази – це окремий вид доказів [4, с. 43]. Цифрові докази вимагають новітніх підходів до їх збирання,

зберігання, використання та дослідження під час доказування у кримінальному провадженні.

У ч. 2 ст. 99 КПК України вказано, що до документів, зокрема, можуть належати «матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані). У ч. 4 ст. 99 КПК України регламентовано, що «дублікат документа, 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 невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа».

Особливої уваги потребує питання щодо отримання інформації з відкритих джерел [5, с. 14, 15; 6]. Це питання постало дуже актуальним під час російсько-української війни і необхідністю фіксації доказів учинення воєнних злочинів. Отримання інформації з відкритих джерел або розвідка відкритих джерел інформації в мережі Інтернет (Open-Source Intelligence - OSINT) передбачає пошук, аналіз та відбір з публічних загальнодоступних джерел певної інформації [7]. Технології та методики OSINT дозволяють отримати якнайбільше потрібної інформації у короткий термін та витрачаючи щонайменше ресурсів [8].

У сучасних джерелах справедливо підкреслюється, що дотримання засади верховенства права передбачає розслідування кримінальних правопорушень і судовий розгляд справ згідно з кращим міжнародним та європейським досвідом [9, с. 79]. Європейські підходи простежуються у пропонуванні переліку (системи) стандартів доказування, які мають застосовуватися під час кримінального провадження («баланс ймовірностей», «перевага доказів», «наявність чітких та перевірених доказів», «поза розумним сумнівом») [10, с. 132–139].

Останнім часом у спеціальних джерелах звертається увага на необхідність впровадження й стандартів розслідування (особливо, що стосується розслідування воєнних злочинів), вироблення певних правил для упорядкування діяльності слідчих (прокурорів). Зокрема, на сьогодні запропоновано «Базові стандарти розслідування для документування міжнародних злочинів в Україні» [11]; «Стандарти розслідування воєнних злочинів. Загальна частина» [12]; «Стандарти розслідування

воєнних злочинів. Незаконне позбавлення волі та катування» [13]; «Основні стандарти розслідування для співробітників служб оперативного реагування при розслідуванні міжнародних злочинів» [14], тощо).

Отримання цифрових доказів має здійснюватися з урахуванням «Керівних принципів щодо електронних доказів», які були прийняті Радою Європи та Державного стандарту України ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» [5, с. 32, 76–123; 15]. Мінімальні стандарти фіксації цифрових доказів (цифрової інформації) встановлює також «Протокол Берклі» (The Berkeley Protocol on Digital Open Source Investigations) [16], який містить положення щодо ефективного використання цифрової інформації: пошуку, збирання, зберігання, перевірки та аналізу даних з відкритих джерел.

Список використаних джерел

1. Докази та доказування у кримінальному провадженні: навч. посібник / Р. І. Благута, Ю. В. Гуцуляк, О. М. Дуфенюк та ін. Львів : ЛьвДУВС, 2018. 272 с.

2. Електронні докази у кримінальному провадженні: поняття, збирання, використання в доказуванні: монографія / І. В. Гора, В. А. Колесник, В. В. Малюк та ін.; за заг. ред. В. А. Колесника. Київ: 7БЦ, 2024. 484 с.

3. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету*. Сер.: Юриспруденція. 2013. № 5. С. 256-260.

4. Метелев О. П. Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства*. 2023. № 1-2. С. 42-53.

5. Вступ до цифрової криміналістики : навч. посіб. / [В. Ю. Шепітько, М. В. Шепітько, К. В. Латиш, М. В. Капустіна, Є. Є. Демидова]; за заг. ред. В. Ю. Шепітька; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2025. 124 с.

6. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень: підручник. Одеса : Юридика, 2024. 180 с.

7. Кожушко О. О. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США. URL: <https://jrnl.nau.edu/index.php/IMV/article/download/3264/3217>

8. Уфімцева О. С. Використання OSINT в умовах збройної агресії РФ проти України. URL: <https://dspace.onua.edu.ua/bitstream/handle/11300/19841/Уфімцева%20Олена%20Сергіївнаopdf?sequence=1&isAllowed=y>
9. Черноус Ю. Вплив міжнародних договорів і практики Європейського суду з прав людини на розвиток криміналістики в Україні. *Право України*. 2021. № 8. С. 77-90.
10. Крет Г. Р. Система стандартів доказування у кримінальному процесі України. *Вісник Південного регіонального центру Національної академії правових наук України*. 2019. № 19. С. 132-139.
11. Basic Investigative Standards for Documenting International Crimes in Ukraine. URL: <https://globalrightscompliance.com/standards-for-documenting-international-crimes-in-ukraine/>
12. Стандарти розслідування воєнних злочинів. *Загальна частина*: метод. рекомендації. затв. 28 квітня 2023 р. Київ, 2023. 112 с.
13. Стандарти розслідування воєнних злочинів. Незаконне позбавлення волі та катування: метод. рекомендації. Затв. 28 квітня 2023 р. Київ, 2023. 102 с. URL: https://justgroup.com.ua/wp-content/uploads/2023/05/standart-rozsliduvannya_katuvannya.pdf
14. Основні стандарти розслідування для співробітників служб оперативного реагування при розслідуванні міжнародних злочинів. URL: www.globalrightscompliance.co.uk; https://martngo.org.ua/wp-content/uploads/2019/04/2016-09-15-10_08_06-1.pdf
15. 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 р. Київ : УкрНДНЦ, 2018. 31 с.
16. 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. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf