DOI https://doi.org/10.30525/978-9934-26-686-7-18

ОКРЕМІ ПРОБЛЕМИ ЦИФРОВОЇ ІНФОРМАЦІЇ ТА ДОСТОВІРНОСТІ, ДОПУСТИМОСТІ ЦИФРОВИХ ДОКАЗІВ

Стратонов В. М., Басиста І. В., Гутник А. В.

ВСТУП

Для формування належної доказової бази надважливо не лише зібрати певну сукупність інформації, а основний акцент слід зробити на таких обставинах, які прогнозовано дозволять такій сукупності відповідати вимогам, які наявні у чинному кримінальному процесуальному законодавстві до доказів.

Отож варто розрізняти терміни «докази» та «інформація». Маємо і такі ситуації (мова про різнопланові порушення), за існування яких є велика доля ймовірності, що здобуто лише інформацію, яка фактично у цьому статусі й залишиться, бо не має шансу іменуватися допустимим та достовірним доказом.

Маємо правову невизначеність у чинному кримінальному процесуальному законодавстві, яка «позбавляє суд та учасників кримінального провадження бути впевненими у правильності правових результатів своїх дій та рішень: щодо електронних (цифрових) доказів – у допустимості цифрової інформації як доказу в кримінальному провадженні»[1]. Частково допомагають практикам поради із Протоколу Берклі, але коли ж слід до нього звертатися?

Сучасний цифровий розвиток дозволяє з упевненістю вести мову не лише про цифрові докази, а й про те, що у найближчому часі виникне необхідність пошуку нових найменувань для інформації, її слідів та доказів[2].

Авторами поставлено собі за мету, на основі аналізу доктринальних підходів, судової практики, наявних практично-орієнтованих порад, не лише окреслити окремі проблеми цифрової інформації та достовірності, допустимості цифрових доказів, а й узагальнити кілька дієвих правил перевірки і підтвердження достовірності цифрової інформації.

---

[1] Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н.В. Глинської ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. С. 274. DOI: https://doi.org/10.31359/9786178612139

[2] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2022. С. 110–112. DOI: https://doi.org/10.31359/9789669982940

Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н.В. Глинської ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. С. 200. DOI: https://doi.org/10.31359/9786178612139

1. Інформація чи докази? Електронна (і), цифрова (і), електронно-цифрова (і)?

Не вперше задаючись таким питанням[3], та як воно вже перебувало у полі зору Афоніна Д.С., Гаврилюк Л.В., Глинської Н.В., Гловюк І.В., Зозулі Н.,

[3] Басиста І.В., Гаврилюк 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: журнал. Серія Право. 2024. Вип. 17 (29). С. 227–243. DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243

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 (30). С. 126–143. DOI: https://doi.org/10.32353/khrife.1.2023.07

Глинська Н. В., Клепка Д. І. Основні аспекти стратегії унормування інституту цифрових доказів в кримінальному процесуальному законодавстві. *Питання боротьби зі злочинністю.* 2023. Вип. 46. С. 49. DOI: https://doi.org/10.31359/2079-6242-2022-46-49

Басиста І.В., Гутник А.В. Цифрова інформація та цифрові докази з відкритих джерел: окремі теоретичні та практичні проблеми. Цифровізація кримінального провадження: стан та перспективи: матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р./ редкол. Н.В. Глинська, Д.І. Клепка, А.А. Барабаш. НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України; від. дослідж. проблем кримін. процесу та судоустрою. Харків: Право, 2024. С. 21–24. DOI: https://doi.org/10.31359/9786178411565

Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / Л.В. Гаврилюк, І.В. Басиста, Д.С. Афонін, А.В. Шевчишен та ін.; за заг. ред. М. С. Цуцкіридзе. Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. 196 с. URL: https://rep.dnuvs.ukr.education/handle/123456789/4178

Басиста І.В., Гутник А.В., Хитра А.Я. Окремі складові до алгоритму процесуальної діяльності залучених у кримінальне провадження уповноважених суб'єктів, які працюють із відкритими джерелами цифрової інформації у перебігу розслідувань, зокрема злочинів проти миру, безпеки людства та міжнародного правопорядку. Українська кримінальна юстиція у пост/воєнній парадигмі: матеріали X (XXIII) Львівського форуму кримінальної юстиції (м. Львів, 19–20 вересня 2024 року) / упорядник І. Б. Газдайка-Василишин. Львів: ЛьвДУВС, 2024. С. 14-20. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/8323/1/19-20_09_2024.pdf

Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: дис. … д-ра філос.: 081 – Право. Львів. держ. ун-т внутр. справ. Львів, 2021. 248 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/3747

Столітній А. В. Електронне кримінальне провадження на досудовому розслідуванні: дис. … д-ра юрид. наук: 12.00.2009. МВС України. Дніпропетров. держ. ун-т внутр. справ. Дніпро, 2018. 648 с.

Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2022. 408 с. DOI: https://doi.org/10.31359/9789669982940

Фоміна Т.Г., Рачинський О.О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник ХНУВС.* 2023. № 3(102). С. 207–220. DOI: https://doi.org/10.32631/v.2023.3.43

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_dokazy__udoskonalennya_ zmin_do_protsesualnogo_zakonodavstva

Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція*. 2013. Вип. 5. С. 256–260. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2013_5_58

Каланчі І.Г., Клепки Д.І., Коваленка А.В., Скрипника А.В., Столітнього А.В., Стратонова В.М., Хитри А.Я, Цехана Д.М. та інших вчених, але і не спостерігаючи певних зрушень у чинному законодавстві, підкреслимо, що очевидно національним орієнтиром у цій царині поки що є лише настанови щодо ідентифікації, збирання, здобуття та збереження цифрових доказів, які містить Національний стандарт України ДСТУ ISO/IEC 27037:2017, який чинний від 01.01.2019 року та покликаний допомогти «організаціям в їхніх дисциплінарних процедурах та забезпеченні обміну потенційними цифровими доказами між юрисдикціями»[4]. Не дивлячись на те, що у інших галузевих законах все ж йде мова про «електронні докази»[5], у аналізованому стандарті згадуються виключно «цифрові докази» і про це вже підкреслювали автори[6]. В силу такого стану справ і у процесуальних документах, і у судових рішеннях, як і у оприлюднених науково-практичних позиціях суддів у слововжитку превалює «електронний»[7], бо передбачувано, що якщо цивільний процесуальний закон оперує цим поняттям, а у кримінальному процесуальному наявна із цього приводу прогалина, то її заповнюють шляхом описаної рецепції. Але така ситуація є не зовсім вірною, про що вже також йшла мова[8].

Зазначений вище стандарт, вміщуючи настанови для роботи із конкретними пристроями, як от: носій для зберігання цифрових даних, використовуваний у стандартних комп'ютерах, мобільні телефони, персональні цифрові помічники персональні електронні прилади (PEDs), карти пам'яті, мобільні

[4] ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). Київ, ДП «УкрДНЦ», 2018. 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf

[5] Цивільний процесуальний кодекс України: Закон України від 18.03.2004 № 1618-IV (зі змін. і доп.). URL: https://zakon.rada.gov.ua/laws/show/1618-15?find=1&text=електронні+#w1_11

[6] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія/ Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2022. С. 74–75, 94. DOI: https://doi.org/10.31359/9789669982940

Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / Л. В. Гаврилюк, І. В. Басиста, Д. С. Афонін, А. В. Шевчишен та ін. ; за заг. ред. М. С. Цуцкіридзе. Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. С. 15. URL: https://rep.dnuvs.ukr.education/handle/123456789/4178

[7] Суддя Верховного Суду Наталія Марчук розповіла про судову практику щодо оцінювання електронних доказів у кримінальному провадженні. *Судово-юридична газета* : веб-сайт. 05.02.2025. URL: https://sud.ua/uk/news/sud-info/322490-sudya-verkhovnogo-suda-natalya-marchuk-rasskazala-o-sudebnoy-praktike-po-otsenke-elektronnykh-dokazatelstv-v-ugolovnom-proizvodstve

Гудима І., Тесля Д., Плугатор Т. Допустити не можна відкинути: як довіряти електронним доказам у кримінальному процесі? *JUSTTALK* : веб-сайт. 06.11.2025. URL: https://justtalk.com.ua/post/dopustiti-ne-mozhna-vidkinuti-yak-doviryati-elektronnim-dokazam-u-kriminalnomu-protsesi

[8] Басиста І.В., Гаврилюк 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: журнал. Серія Право.* 2024. Вип. 17 (29). С. 230. DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243

навігаційні системи, цифрові фото- та відеокамери, стандартний комп'ютер з мережевими з'єднаннями; мережі, які ґрунтовані на TCP/IP та інших цифрових протоколах, а також прилади з функціями, подібними наведеним вище[9], все ж підкреслює, що запропонований перелік не претендує на вичерпність[10] і це логічне, у силу розвитку технологій. При цьому, у стандарті йдеться виключно про «цифровість», хоча, згоджуємося, що очевидно згодом з'являться не лише «нові види пристроїв, але і нові типи запису інформації»[11], як і її передавання[12], що зумовить пошук нових найменувань для інформації, її слідів та доказів. При цьому поділяємо наукову позицію щодо виокремлення окремого джерела таких цифрових доказів[13]. Також розділяємо процесуальні хвилювання тих наших колег, які аргументовано підкреслюють, що «відсутність належної правової регламентації певного правового явища, зокрема електронних (цифрових) доказів є окремим ризиком у правозастосуванні, оскільки правова невизначеність позбавляє суд та учасників кримінального провадження бути впевненими у правильності правових результатів своїх дій та рішень: щодо електронних (цифрових) доказів – у допустимості цифрової інформації як доказу в кримінальному провадженні»[14].

Ще однією спірною ситуацією є ототожнення цифрової інформації та цифрових доказів. У будь-якому випадку жодна інформація одразу не здатна набути процесуального статусу доказу у кримінальному провадженні. Цифрова інформація не є винятком. Лише перевірена та достовірна інформація, яка відповідає вимогам належності та допустимості, отримана в передбаченому КПК України порядку та може бути використана для встановлення наявності чи відсутності фактів та обставин, що мають значення для кримінального провадження і підлягають доказуванню[15] має «процесуальний шанс»

[9] ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). Київ, ДП «УкрДНЦ», 2018. 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf

[10] Там само.

[11] Фоміна Т.Г., Рачинський О.О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник ХНУВС*. 2023. № 3(102). С. 209–210. DOI: https://doi.org/10.32631/v.2023.3.43

[12] Коваленко А.В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник ЛДУВС ім. Е. О. Дідоренка.* 2022. Вип. 4 (100). С. 233. https://doi.org/10.33766/2524-0323.100.226-236

[13] Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2022. С. 110–112. DOI: https://doi.org/10.31359/9789669982940

Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н.В. Глинської ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. С. 200. DOI: https://doi.org/10.31359/9786178612139

[14] Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н.В. Глинської ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. С. 274. DOI: https://doi.org/10.31359/9786178612139

[15] Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 року № 4651-VI (зі змін. і доп.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

іменуватися доказом. Отож варто розрізняти терміни «докази» та «інформація». Маємо і такі ситуації, за яких несанкціонований доступ до інформації, викрадення облікових записів, порушення умов надання послуг, як от користувацької угоди щодо веб-сайту або платформи, скрейпінг (коли це заборонено певною юрисдикцією) тощо унеможливлять набуття нею статусу доказу у кримінальному провадженні, тобто інформацію ми здобудемо, а допустимий та достовірний доказ – ні[16].

2. Достовірність та допустимість, як досягнути?

Здавалось би, такий процес збору інформації є не складним, проте нами вже була встановлена ціла низка наявних труднощів, зокрема і щодо помилкових підходів до збору цифрової інформації загалом, та із відкритих джерел, зокрема, ланцюга її збереження, відсутності спеціальних критеріїв для її оцінки тощо[17], виходячи із тих вимог, які окрім КПК України наявні і у Протоколі Берклі[18]. Дослідниці навіть запропонували вирішити проблеми із цифровими доказами через комплексний крок законодавця, як от Закон України «Про внесення змін до Кримінального процесуального кодексу України щодо цифровізації кримінального провадження» та підготували і оприлюднили відповідну пояснювальну записка до його проєкту[19].

Суддя Верховного Суду, розповідаючи про судову практику щодо оцінювання електронних доказів у кримінальному провадженні в рамках курсу HELP «Кіберзлочинність та електронні докази», серед іншого важливого, підкреслювала, що не маловажливою є якість таких доказів, йшлося

---

[16] Басиста І.В., Гутник А.В. Цифрова інформація та *цифрові докази з відкритих джерел: окремі теоретичні та практичні проблеми. Цифровізація кримінального провадження: стан та перспективи*: матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р./ редкол. Н.В. Глинська, Д.І. Клепка, А.А. Барабаш. НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України; від. дослідж. проблем кримін. процесу та судоустрою. Харків: Право, 2024. С. 21–24. DOI: https://doi.org/10.31359/9786178411565

[17] Басиста І.В., Гаврилюк 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* : журнал. *Серія Право*. 2024. Вип. 17 (29). С. 229. DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243

[18] Протокол Берклі з ведення розслідування 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; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-ProtocolUkrainian.pdf

[19] Глинська Н.В., Клепка Д.І. Пропозиції до чинного кримінального процесуального законодавства України. Цифровізація кримінального провадження: стан та перспективи : матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р. / [редкол.: Н. В. Глинська (голов. ред.), Д.І. Клепка, А. А. Барабаш] ; НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України ; Від. дослідж. проблем кримін. процесу та судоустрою. Харків : Право, 2024. С. 165–173. DOI: https://doi.org/10.31359/9786178411565

безпосередньо про якість відеозапису. Також акцентовано, що «дублікат документа, а також копії інформації, у тому числі комп'ютерних даних, що містяться в інформаційних (автоматизованих) системах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа. Прокурор має обґрунтувати походження електронних доказів та інші процесуальні питання, які стосуються наданих ним електронних доказів»[20].

Також судді звертають увагу на часті звернення сторони захисту, тобто клопотання про недопустимість таких доказів через те, що «певний файл кілька разів копіювався на різні носії (особливо якщо також змінювався формат цифрових даних), а тому він не є оригіналом і його цілісність порушено»[21]. І з цього приводу правильно підмічено, що за описаної ситуації сумнів має стосуватися не допустимості, а «достовірності (автентичності): чи дійсно електронний доказ є справжнім і чи можна йому довіряти»?[22]

І у продовження цілком вірно діагностовано про те, що для доведення достовірності доказу (принаймні відсутності втручання з боку сторони обвинувачення) має спосіб документування і забезпечення безперервності контролю над доказами з моменту їх отримання і до моменту їх дослідження в суді (тобто те, що в англомовній літературі називають «chain of custody», тобто ланцюг забезпечення зберігання речових доказів під час їх поетапної передачі, який має усунути будь-які розумні сумніви щодо можливої підробки з боку правоохоронців). На жаль, вітчизняна практика судів першої інстанції з аналізу ланцюга зберігання електронних доказів не є поширеною і поняття «chain of custody» рідко фігурує в рішеннях»[23].

У 2024 році авторським колективом науково-практичного порадника «Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі)», серед інших важливих порад для представників органів досудового розслідування, підкреслювалося про складові кожного із етапів chain of custody та його важливості загалом для набуття здобутою інформацією статусу доказу

[20] Суддя Верховного Суду Наталія Марчук розповіла про судову практику щодо оцінювання електронних доказів у кримінальному провадженні. *Судово-юридична газета* : веб-сайт. 05.02.2025. URL: https://sud.ua/uk/news/sud-info/322490-sudya-verkhovnogo-suda-natalya-marchuk-rasskazala-o-sudebnoy-praktike-po-otsenke-elektronnykh-dokazatelstv-v-ugolovnom-proizvodstve

[21] Гудима І., Тесля Д., Плугатор Т. Допустити не можна відкинути: як довіряти електронним доказам у кримінальному процесі? *JUSTTALK* : веб-сайт. 06.11.2025. URL: https://justtalk.com.ua/post/dopustiti-ne-mozhna-vidkinuti-yak-doviryati-elektronnim-dokazam-u-kriminalnomu-protsesi

Судді ККС ВС обговорили *проблемні питання допустимості електронних доказів під час судового розгляду. Верховний Суд* : веб-сайт. 28.10.2021. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/

[22] Гудима І., Тесля Д., Плугатор Т. Допустити не можна відкинути: як довіряти електронним доказам у кримінальному процесі? *JUSTTALK* : веб-сайт. 06.11.2025. URL: https://justtalk.com.ua/post/dopustiti-ne-mozhna-vidkinuti-yak-doviryati-elektronnim-dokazam-u-kriminalnomu-protsesi

[23] Там само.

у кримінальному провадженні[24]. І за ситуації дотримання всіх пропонованих рекомендацій отримаємо серед іншого процесуально-бажаного і процесуальну економію, адже під час правильного отримання цифрової інформації та належного поводження із нею взагалі може відпасти будь-яка потреба в призначенні та проведенні експертиз, бо саме такою є наявна практика Верховного Суду[25]. Вірно помітили автори, що через обраний підхід колегією суддів Третьої судової палати ККС ВС від 12.06.2024 у справі № 569/1908/23, для сторін сформувалася «чітка інструкція: якщо вони бажають заявити про недостовірність електронного доказу, таке питання може вирішуватися через проведення експертизи»[26]. Звісно є й такі ситуації у перебігу досудового розслідування та й судового розгляду, коли без проведення експертизи не обійтися, зокрема це пов'язане із deepfakes, участі ШІ тощо, про що теж більш розлоге вже йшлося[27].

З огляду значної кількості не вирішених проблем у цій царині вже навіть на монографічному рівні І.Г. Каланча запропонувала, серед іншого нагального, і комплекс алгоритмів пошуку та фіксації цифрових доказів та методику підтвердження їх автентичності та цілісності, вживаючи їх означення через словосполучення «докази електронної форми»[28].

Цікавим є досвід інших країн щодо використання цифрових доказів у кримінальному судочинстві. Г. Авдєєва та Е. Живуцька-Козловська встановили, що на сьогодні у США діють Federal Rules of Evidence[29], які

---

[24] Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / Л. В. Гаврилюк, І. В. Басиста, Д. С. Афонін, А. В. Шевчишен та ін. ; за заг. ред. М. С. Цуцкіридзе. Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. 196 с. https://rep.dnuvs.ukr.education/handle/123456789/4178

[25] Постанова колегії суддів Третьої судової палати ККС ВС від 12.06.2024 у справі № 569/1908/23.URL: https://reyestr.court.gov.ua/Review/119741340

[26] Гудима І., Тесля Д., Плугатор Т. Допустити не можна відкинути: як довіряти електронним доказам у кримінальному процесі? JUSTTALK : веб-сайт. 06.11.2025. URL: https://justtalk.com.ua/post/dopustiti-ne-mozhna-vidkinuti-yak-doviryati-elektronnim-dokazam-u-kriminalnomu-protsesi

[27] Басиста І.В., Гутник А.В., Хитра А.Я. Розпізнавання deepfakes як домінантна складова протидії інформаційним загрозам. Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : тези III Міжнародної науково-практичної конференції (Хмельницький, 21 листопада 2024 року). Хмельницький : Видавництво НАДПСУ, 2025. С. 1097–1099.

Басиста І.В. Використання ШІ в криміналістичних цілях та співвіднесення із допустимістю зібраних доказів: огляд сучасного стану справ: розділ до монографії «Нове століття криміналістики та судових наук : Liber Amicorum на честь академіка В. Ю. Шепітька»: монографія / [М. Шепітько, А. Гетьман, В. Журавель та ін.] ; Нац. юрид. ун-т ім. Ярослава Мудрого ; Нац. акад. прав. наук України ; Міжнар. конгрес криміналістів ; [за ред. М. В. Шепітька]. Харків : Право, 2026. С. 388–405. URL: https://dspace.nlu.edu.ua/handle/123456789/20701

[28] Каланча І.Г. Докази електронної форми у кримінальному процесі України: теорія та практика. Дисертація на здоб. ступеня д.ю.н. спец. 12.00.09. Національна академія внутрішніх справ, Київ, 2025. С. 34–35 та ін. https://elar.navs.edu.ua/handle/123456789/38317

[29] Federal Rules of Evidence amended to December 1, 2024. Legal Information Institute. URL: https://www.law.cornell.edu/rules/fre

кільканадцять разів змінювали та доповнювали. Опитуванням практиків у США було встановлено, що їм також «не вистачає знань про технічні характеристики цифрової інформації, правила її вилучення та зберігання. Слідчі потребують комплектів науково-технічних засобів для роботи з цифровими доказами, зокрема сумок Фарадея для ізолювання електронних пристроїв»[30]. При цьому важливо, що на відміну від нашого стану справ, ще «наприкінці XX ст. цифрові докази у США виокремили у групу доказів у зв'язку з особливостями їх створення, зберігання, виявлення, дослідження й оцінки їх допустимості та достовірності. 1995 р. спільними зусиллями правоохоронні органи США, Канади й деяких країн Європи створили міжнародну організацію з комп'ютерних доказів (англ. International Organization on Computer Evidence, IOCE)[31], а 1998 р.– Наукову робочу групу з дослідження цифрових доказів (англ. Scientific Working Group on Digital Evidence, далі – SWGDE)[32], яка об'єднала роботу правоохоронних, академічних і комерційних організацій у галузі цифрової криміналістики з метою розроблення міждисциплінарних посібників і стандартів щодо відновлення, збереження й дослідження цифрових доказів. Група SWGDE розробила основні стандарти та принципи роботи з цифровими доказами, що забезпечує належність і допустимість цих доказів у судочинстві»[33].

Із Federal Rules of Evidence (https://www.law.cornell.edu/rules/fre) слідує важливе правило, яке також констатоване і вище цитованими авторками та котре, на жаль, нехтується у національних розслідуваннях та судових розглядах, про допущення до дослідження цифрових доказів лише кваліфікованих IT-спеціалістів із метою максимального збереження їх цілісності[34].

3. Перевірка і підтвердження достовірності цифрової інформації

Перевірка достовірності цифрової інформації як елемент її доказового значення не є унікальною для кримінального процесу. У суміжних сферах (журналістика, OSINT, аналітика відкритих джерел) вже сформовані сталі підходи до верифікації цифрового контенту, які можуть бути адаптовані до потреб кримінального провадження. Наприклад, Етичний кодекс українського журналіста визначає, що найпершим обов'язком журналіста є повага до права громадськості на повну та об'єктивну інформацію про факти та події. Будь-яка тема потребує максимально повного набору фактів і думок. Тому завдання

[30] 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 (30). С. 126–143. DOI: https://doi.org/10.32353/khrife.1.2023.07

[31] International Organization on Computer Evidence (IOCE) / UIA. Global Civil Society Database. URL: https://uia.org/s/or/en/1100029648

[32] Scientific Working Group on Digital Evidence (SWGDE). URL: https://www.swgde.org/

[33] 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 (30). С. 126–143. DOI: https://doi.org/10.32353/khrife.1.2023.07

[34] Там само.

журналіста все це знайти в компетентних джерелах[35]. Серед ключових принципів медіаграмотності є «правило трьох джерел». Це правило зводиться до перевірки інформації у мінімум трьох різних (за назвою, формою власності, редакційною політикою, географічним розташуванням) джерелах[36]. Схожий принцип використовують OSINTери – «трикутник перевірки» (Verification Triangle). Суть підходу – перевірити інформацію щонайменше з трьох різних джерел або точок зору: (1) оригінальні документи чи офіційні дані; (2) незалежні відкриті джерела (новини, бази даних, свідки); (3) технічні чи цифрові підтвердження (геолокація, метадані, фото/відеоаналіз). Тільки коли трикутник «замикається» – можна говорити, що факт підтверджено. Автори наводять приклад, що для початку аналізують джерело публікації, далі шукають інші підтвердження, на останок здійснюють цифрову перевірку [37].

Способи перевірки цифрової інформації на достовірність у кримінальному провадженні також надавались нами раніше[38]. Аналізуючи достовірність результатів OSINT у судовій практиці, І. Головюк пропонує під час роботи з відкритими джерелами визначити, чи є інформація або твердження в цифровому контенті на перший погляд надійними, шляхом перегляду та оцінки контенту, а також контекстуальної інформації, що міститься у файлі. Зокрема, це перевірка вбудованих метаданих, пов'язаної інформації та джерела. Цей процес повинен включати спробу ідентифікувати оригінальне джерело матеріалу, що може вимагати відстеження походження даних в Інтернеті, особи, яка завантажила їх, або автора[39].

Тож, з урахуванням цих висновків, з метою підтвердження чи спростування достовірності цифрової інформації пропонуємо адаптований під кримінальне провадження «трикутник перевірки» цифрової інформації на достовірність. Запропонований нами підхід фактично формує рівневу модель перевірки

---

[35] Кодекс етики українського журналіста. *Комісія журналістської етики* : веб-сайт. URL: https://cje.org.ua/ethics-codex/?fbclid=IwY2xjawPJ59NleHRuA2FlbQIxMABicmlkETF4d1FuTWloZlk1T3ZEN1pwc3J0YwZhcHBfaWQQMjIyMDM5MTc4ODIwMDg5MgABHsqw8h9Oh1aWfNOZBnZqXuxSBrJIRYAiNvwPx76s8XnuKMKV4mdz3vTw1Xb0_aem_YGU4piOQHM4oz1Zfvz92Jw

[36] Майданюк В. Правило трьох джерел: чому важливо перевіряти інформацію з різних, незалежних джерел. *Онлайн-медіа Дослідницько-аналітичної групи «ІнфоЛайт»*. 29.05.2025. URL: https://infolight.in.ua/2025/05/29/pravylo-troh-dzherel-chomu-vazhlyvo-pereviryaty-informatsiyu-z-riznyh-nezalezhnyh-dzherel/

[37] Трикутник перевірки інформації в OSINT: як відрізнити факт від маніпуляції. *InsightOps* : веб-сайт. 26.08.2025. URL: https://insightops.com.ua/2025/08/26/%D1%82%D1%80%D0%B8%D0%BA%D1%83%D1%82%D0%BD%D0%B8%D0%BA-%D0%BF%D0%B5%D1%80%D0%B5%D0%B2%D1%96%D1%80%D0%BA%D0%B8-%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97-%D0%B2-osint-%D1%8F%D0%BA/

[38] Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванн : колективна монографія / А. В. Гутник, А. Я. Хитра. Львів : ЛьвДУВС, 2022. С. 100.

[39] Головюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* 2025. Випуск 91: частина 4. С. 255. DOI https://doi.org/10.24144/2307-3322.2025.91.4.35

цифрової інформації, яка охоплює як змістовну, так і технічну складову цифрового доказу.

Першим кроком є *перевірка джерела публікації.* Що розуміти під «аналізом джерела» пояснено у п.177 Протоколу Берклі. Рекомендації щодо ідентифікації і перевірки першоджерела і змісту (включаючи місце події, дату і приблизний час) можна знайти у Посібнику з Верифікації[40].

У цьому блоці звернемо увагу тільки щодо проблем встановлення автора цифрової інформації. Так, у п. 177 Протоколу Берклі зазначено, що «…Інтернет-середовище створює труднощі для аналізу джерел, оскільки багато джерел є анонімними або псевдонімними …[41]. Наприклад, є випадки, коли автор цифрової інформації видає себе за іншу особу. Так, підозрюваний з метою приховання вбивства та дезорієнтації правоохоронних органів організував поїздку до Єгипту, штучно створивши собі алібі щодо перебування за межами України у момент вчинення злочину. Перебуваючи в м. Шарм-ель-Шейх, він від імені потерпілого публікував повідомлення та фото в соціальній мережі Фейсбук, які мали створити уявлення, що потерпілий живий і самостійно залишив територію України, чим намагався приховати реальну дату та обставини вчинення вбивства[42]. Аналізуючи цю ухвалу у іншому дослідженні, ми висловлювали свої застереження що використання одного ізольованого доказу, зокрема даних про місце перебування особи, є недостатнім для достовірного підтвердження алібі та потребує перевірки у сукупності з іншими доказами[43].

Можуть бути і інші ситуації, наприклад коли цифрова інформація публікується від імені фейкової особи. Наприклад, у січні 2024 року з метою компрометації журналістів створено фейкове видання, у редакції якого зазначено вигаданих осіб з фотографіями, які згенерував штучний інтелект[44]. Публікація від імені вигаданої особи це те ж саме що і публікація від імені невідомої особи. Також уважно слід відноситись до баз-даних, які невідомо ким створені та адмініструються. Наприклад, база-даних «Миротворець». Дані з цієї мережі можуть не відповідати, окрім інших вимог, вимозі достовірності (неможливо

[40] Посібник з Верифікації. Редактор: Крейг Сільверман, Інститут Пойнтера. Редагування та адаптацію перекладу на українську мову здійснено Українською Асоціацією Видавців під керівництвом Олексія Погорелова Переклад, літературне редагування та верстка В'ячеслав Білоусов Фінальна верстка – Європейський центр журналістики. С. 106–109. URL: https://verificationhandbook.com/downloads/verification.handbook_ua.pdf

[41] Протокол Берклі з ведення розслідування 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; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. С. 92. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-ProtocolUkrainian.pdf

[42] Ухвала Печерського районного суду м. Києва від 17.03.2016 року у справі № 757/12089/16-к. URL: http://reyestr.court.gov. ua/Review/56950544

[43] Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : колективна монографія / А. В. Гутник, А. Я. Хитра. Львів : ЛьвДУВС, 2022. С. 56.

[44] Романюк А. Метод «гнилого оселедця»: хто і навіщо атакує журналістів. *Детектор медіа* : веб-сайт. 16.01.2025. URL: https://detector.media/blogs/article/221791/2024-01-16-metod-gnylogo-oseledtsya-khto-i-navishcho-atakuie-zhurnalistiv/

встановити хто, коли та для чого публікував інформацію, яка лежить в основі досьє, хто наповнює базу)[45]. Є також випадки, коли власник сайту відомий, однак, через співпрацю з анонімними джерелами виникають сумніви щодо достовірності інформації. Наприклад, приватний сайт-парсер YouControl, який раніше використовував у своїй роботі тільки державні реєстри додав базу даних «Миротворець». Тож використання інформації із таких баз даних для доказування несе певні ризики[46]. Аналогічно, неможливо беззастережно довіряти інформації, опублікованій ворогом, адже є непоодинокі випадки викривлення чи вигадання інформації, яка публікується на його офіційних сайтах.

У п. 177 Протоколу Берклі також зазначено, що хоча визначення авторства є корисним, втім його відсутність, як правило, не є критичним для встановлення автентичності онлайн-елемента[47]. Таким чином, у сучасних міжнародних підходах акцент зміщується з ідентифікації автора цифрового контенту на встановлення автентичності самого цифрового об'єкта та цілісності інформації. Однак, у деяких категоріях кримінальних правопорушень, зокрема під час перевірки достовірності відео жорстокого поводження над твариною, встановлення особи автора є однією із обставин, що підлягає доказуванню.

Наступним кроком є пошук *підтвердження у інших джерелах*. Для цього слід провести слідчі або негласні (слідчі) розшукові дії. Також можна перевірити доказову інформацію з використанням відкритих джерел (медіа, соціальні медіа, веб-сайти, бази даних, офіційні дані тощо[48]). Під час пошуку підтверджень у інших джерелах, як ми зазначали вище, у журналістів є стандарт перевірки якнайменше в трьох різних джерелах[49].

---

[45] Басиста І., Гутник А. Використання інформації з бази даних Центру «Миротворець» у перебігу досудового розслідування: окремі аспекти. *Держава і суспільство: сучасні виклики та пошук рішень* : Збірник матеріалів III Всеукраїнської науково-теоретичної конференції, 16 травня 2024 р. К.: КТГГ, 2024. С. 397.

[46] Басиста І.В., Гутник А.В. Цифрова інформація та цифрові докази з відритих джерел: окремі теоретичні та практичні проблеми. *Цифровізація кримінального провадження: стан та перспективи* : матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р. / [редкол.: Н. В . Глинська (голов. ред.), Д. І . Клепка, А. А . Барабаш] ; НДІ вивч. проблем злочинності ім. акад. В. В . С ташиса НАП рН України ; Від. дослідж. проблем кримін. процесу та судоустрою. Харків : Право, 2024. С. 21.

[47] Протокол Берклі з ведення розслідування 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; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. С. 92. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-ProtocolUkrainian.pdf

[48] Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / Л. В. Гаврилюк, І. В. Басиста, Д. С. Афонін, А. В. Шевчишен та ін. ; за заг. ред. М. С. Цуцкірідзе. Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. С. 23–30. URL: https://rep.dnuvs.ukr.education/handle/123456789/4178

[49] Посібник з Верифікації. Редактор: Крейг Сільверман, Інститут Пойнтера. Редагування та адаптацію перекладу на українську мову здійснено Українською Асоціацією Видавців під керівництвом Олексія Погорелова. Переклад, літературне редагування та верстка – В'ячеслав Білоусов. Фінальна верстка – Європейський центр журналістики. С. 105. URL: https://verificationhandbook.com/downloads/verification.handbook_ua.pdf

Підтвердження певної інформації можна знайти у матеріалах журналістських розслідувань. Наприклад, на підставі фактів, оприлюднених у журналістському розслідуванні щодо діяльності на території одного з монастирів Голосіївського району міста Києва підпільного навчального закладу СБУ розпочали досудове розслідування за ч. 1 ст. 436-1 КК[50].

Однак, для того, щоб ця інформація стала доказом, її слід «легалізувати». Уповноважений суб'єкт має фактично повторно її зібрати за допомогою засобів і способів, що визначені КПК. Орієнтовний алгоритм «легалізації» матеріалів журналістського розслідування та блогів пропонує А. Коваленко. Автор резонно зазначає, що матеріал журналістського розслідування перед використанням повинен бути оціненим з точки зору належності, допустимості і достовірності[51]. Адже опублікованими можуть бути замовні чи неправдиві матеріали.

Закінченням перевірки є *цифрова перевірка.* Сюди можна віднести технічний аналіз та верифікацію метаданих[52], дослідження хеш-значень для підтвердження цілісності, оцінка технічних параметрів пристрою, експертиза тощо. Про деякі із цих процесів вже йшла мова у попередньому підрозділі.

ВИСНОВКИ

Отож, інформація одразу не здатна набути процесуального статусу доказу у кримінальному провадженні. Цифрова інформація не є винятком. Лише перевірена та достовірна інформація, яка відповідає вимогам належності та допустимості, отримана в передбаченому КПК України порядку та може бути використана для встановлення наявності чи відсутності фактів та обставин, що мають значення для кримінального провадження і підлягають доказуванню має «процесуальний шанс» іменуватися доказом. При цьому, кваліфіковані ІТ-спеціалісти повинні залучатися на допомогу слідчому, детективу до відповідних оглядів, обшуків, для відшукання цифрових слідів тощо.

Розділяємо наукову позицію щодо виокремлення окремого джерела цифрових доказів та про правову невизначеність у кримінальному процесуальному законодавстві у царині допустимості цифрової інформації, як доказу в кримінальному провадженні.

Перевірка і підтвердження достовірності цифрової інформації у кримінальному провадженні має здійснюватися як багаторівневий процес, що поєднує аналіз джерела, пошук підтверджень у незалежних джерелах та технічну (цифрову) перевірку. Адаптація підходів, сформованих у журналістиці, OSINT, до вимог кримінального процесу дозволяє мінімізувати ризики використання недостовірних даних.

---

[50] Розпочато досудове розслідування за фактами, *оприлюдненими журналістами Слідство.Інфо, щодо підпільної школи на території монастиря. Офіс Генерального прокурора* : веб-сайт. 07.01.2026. URL: https://gp.gov.ua/ua/posts/rozpocato-dosudove-rozsliduvannya-za-faktami-oprilyudnenimi-zurnalistami-slidstvoinfo-shhodo-pidpilnoyi-skoli-na-teritoriyi-monastirya

[51] Розслідування колабораційної діяльності : практ. посібник / Є.О. Письменський, С.В. Головкін, А.В. Коваленко, В.В. Коваленко. Київ: ВД Дакор, 2024. С. 182–183.

[52] Главюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету*, 2025. *Серія ПРАВО*. Випуск 91: частина 4. С. 257. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.35

АНОТАЦІЯ

Запропонована публікація є продовженням серії авторських науково-практичних роздумів щодо розмежування сукупності інформації від сукупності доказів. Вкотре аргументовано, що екстраполюючи ці висновки на цифрову інформацію, варто не лише знати межу, яка відділяє цифрову інформацію від статусу цифрового доказу, а й розуміти, як уникати тих процесуальних та інших порушень, які не дозволять цифровій інформації іменуватися допустимим та достовірним доказом.

Зроблено спробу частково заповнити правову невизначеність, яка має місце у чинному кримінальному процесуальному законодавстві, порадами із Протоколу Берклі задля забезпечення допустимості цифрової інформації, як доказу в кримінальному провадженні. Також узагальнено кілька дієвих правил перевірки і підтвердження достовірності цифрової інформації та продовжено прогнози щодо наслідків сучасного цифрового розвитку для доказового права загалом та кримінальної процесуальної діяльності зі збору, перевірки та оцінки цифрової інформації зокрема.

Література

1. Federal Rules of Evidence amended to December 1, 2024. Legal Information Institute. URL: https://www.law.cornell.edu/rules/fre

2. International Organization on Computer Evidence (IOCE) / UIA. Global Civil Society Database. URL: https://uia.org/s/or/en/1100029648

3. Scientific Working Group on Digital Evidence (SWGDE). URL: https://www.swgde.org/

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 (30). С. 126–143. DOI: https://doi.org/10.32353/khrife.1.2023.07

5. Басиста І., Гутник А. Використання інформації з бази даних Центру «Миротворець» у перебігу досудового розслідування: окремі аспекти. *Держава і суспільство: сучасні виклики та пошук рішень:* Збірник матеріалів ІІІ Всеукраїнської науково-теоретичної конференції, 16 травня 2024 р. К.: КТГГ, 2024. С. 395–398.

6. Басиста І.В. Використання ШІ в криміналістичних цілях та співвіднесення із допустимістю зібраних доказів: огляд сучасного стану справ: розділ до монографії «Нове століття криміналістики та судових наук : Liber Amicorum на честь академіка В. Ю. Шепітька»: монографія / [М. Шепітько, А. Гетьман, В. Журавель та ін.] ; Нац. юрид. ун-т ім. Ярослава Мудрого ; Нац. акад. прав. наук України ; Міжнар. конгрес криміналістів ; [за ред. М.В. Шепітька]. Харків : Право, 2026. С. 388–405. URL: https://dspace.nlu.edu.ua/handle/123456789/20701

7. Басиста І.В., Гаврилюк 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: журнал. Серія Право.* 2024. Вип. 17 (29). С. 227–243. DOI: https://doi.org/10.33098/2078-6670.2024.17.29.227-243

8. Басиста І.В., Гутник А.В. Цифрова інформація та цифрові докази з відкритих джерел: окремі теоретичні та практичні проблеми. *Цифровізація кримінального провадження:* стан та перспективи : матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р./ редкол. Н.В. Глинська, Д.І. Клепка, А.А. Барабаш. НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України; від. дослідж. проблем кримін. процесу та судоустрою. Харків: Право, 2024. С. 21–24. DOI: https://doi.org/10.31359/9786178411565

9. Басиста І.В., Гутник А.В., Хитра А.Я. Окремі складові до алгоритму процесуальної діяльності залучених у кримінальне провадження уповноважених суб'єктів, які працюють із відкритими джерелами цифрової інформації у перебігу розслідувань, зокрема злочинів проти миру, безпеки людства та міжнародного правопорядку. *Українська кримінальна юстиція у пост/воєнній парадигмі:* матеріали X (XXIII) Львівського форуму кримінальної юстиції (м. Львів, 19–20 вересня 2024 року) / упорядник І. Б. Газдайка-Василишин. Львів: ЛьвДУВС, 2024. С. 14-20. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/8323/1/19-20_09_2024.pdf (дата звернення: 19.01.2026).

10. Басиста І.В., Гутник А.В., Хитра А.Я. Розпізнавання deepfakes як домінантна складова протидії інформаційним загрозам. *Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану :* тези III Міжнародної науково-практичної конференції (Хмельницький, 21 листопада 2024 року). Хмельницький : Видавництво НАДПСУ, 2025. С. 1097–1099.

11. Басиста І.В., Дроздов О.М., Стратонов В.М. Провадження за нововиявленими обставинами та провадження за виключними обставинами. Особливості, перебіг та взаємозв'язок. *Науковий вісник Херсонського державного університету. Серія юридичні науки Випуск 2 Гельветика, 2023.* С. 10. https://lj.journal.kspu.edu/index.php/lj/issue/view/ 11/55 (дата звернення: 19.01.2026).

12. Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / Л. В. Гаврилюк, І. В. Басиста, Д. С. Афонін, А. В. Шевчишен та ін. ; за заг. ред. М. С. Цуцкірідзе. Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. 196 с. URL: https://rep.dnuvs.ukr.education/handle/123456789/4178 (дата звернення: 19.01.2026).

13. Глинська Н. В., Клепка Д. І. Основні аспекти стратегії унормування інституту цифрових доказів в кримінальному процесуальному законодавстві. *Питання боротьби зі злочинністю.* 2023. Вип. 46. С. 48–66. DOI: https://doi.org/10.31359/2079-6242- 2022-46-49 (дата звернення: 19.01.2026).

14. Глинська Н.В., Клепка Д.І. Пропозиції до чинного кримінального процесуального законодавства України. *Цифровізація кримінального провадження: стан та перспективи :* матеріали наук.-практ. круглого столу, м. Харків, 19 верес. 2024 р. / [редкол.: Н. В. Глинська (голов. ред.), Д.І. Клепка, А. А. Барабаш] ; НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України ; Від. дослідж. проблем кримін. процесу та судоустрою. Харків : Право, 2024. С. 165–173. DOI: https://doi.org/10.31359/9786178411565 (дата звернення: 19.01.2026).

15. Главюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* 2025. Випуск 91: частина 4. С. 251–259. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.35 (дата звернення: 19.01.2026).

16. Гудима І., Тесля Д., Плугатор Т. Допустити не можна відкинути: як довіряти електронним доказам у кримінальному процесі? *JUSTTALK* : веб-сайт. 06.11.2025. URL: https://justtalk.com.ua/post/dopustiti-ne-mozhna-vidkinuti-yak-doviryati-elektronnim-dokazam-u-kriminalnomu-protsesi (дата звернення: 19.01.2026).

17. Military offences and war crimes: background, theory and practice / Ed. by V.M. Stratonov. – Riga, Latvia: «Baltija Publishing», 2023. 876 p

18. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). Київ, ДП «УкрДНЦ», 2018. 31 с. URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf

19. 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_dokazy__udoskonalennya_zmin_do_protsesualnogo_zakonodavstva (дата звернення: 19.01.2026).

20. Каланча І.Г. Докази електронної форми у кримінальному процесі України: теорія та практика. Дисертація на здоб. ступеня д.ю.н. спец. 12.00.09. Національна академія внутрішніх справ, Київ, 2025. 617 с. URL: https://elar.navs.edu.ua/handle/123456789/38317

21. Коваленко А.В. Поняття та сутність електронних (цифрових) слідів кримінального правопорушення. *Вісник ЛДУВС ім. Е. О. Дідоренка.* 2022. Вип. 4 (100). С. 226–236. DOI: https://doi.org/10.33766/2524-0323.100.226-236

22. Кодекс етики українського журналіста. *Комісія журналістської етики :* веб-сайт. URL: https://cje.org.ua/ethics-codex/?fbclid=IwY2xjaw PJ59NleHRuA2FlbQIxMABicmlkETF4d1FuTWloZlk1T3ZEN1pwc3J0YwZhcHBfaWQQMjIyMDM5MTc4ODIwMDg5MgABHsqw8h9Oh1aWfNOZBnZqXuxSBrJIRYAiNvwPx76s8XnuKMKV4mdz3vTw1Xb0_aem_YGU4piOQHM4oz1Zfvz92Jw

23. Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н.В. Глинської ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. 452 с. DOI: https://doi.org/10.31359/9786178612139

24. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 року № 4651-VI (зі змін. і доп.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

25. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: колективна монографія / А. В. Гутник, А. Я. Хитра. Львів : ЛьвДУВС, 2022. 204 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/%D0%93%D1%83%D1%82%D0%BD%D0%B8%D0%BA%2C%20%D0%A5%D0%B8%D1%82%D1%80%D0%B0_%D0%BC%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F_21_06_2022.pdf

26. Майданюк В. Правило трьох джерел: чому важливо перевіряти інформацію з різних, незалежних джерел. *Онлайн-медіа Дослідницько-*

аналітичної групи «ІнфоЛайт» : веб-сайт. 29.05.2025. URL: https://infolight.in.ua/2025/05/29/pravylo-troh-dzherel-chomu-vazhlyvo-pereviryaty-informatsiyu-z-riznyh-nezalezhnyh-dzherel/ (дата звернення: 19.01.2026).

27. Науково-практичний коментар Кримінального процесуального кодексу України – науково-методична робота. Станом на 14 квітня 2024 року / За заг. ред. Стратонова В.М. Київ: Видавничий дім «Професіонал», 2024. 1208 с. (дата звернення: 19.01.2026).

28. Посібник з Верифікації. Редактор: Крейг Сільверман, Інститут Пойнтера. Редагування та адаптацію перекладу на українську мову здійснено Українською Асоціацією Видавців під керівництвом Олексія Погорелова Переклад, літературне редагування та верстка – В'ячеслав Білоусов Фінальна верстка – Європейський центр журналістики. 130 с. URL: https://verificationhandbook.com/downloads/verification.handbook_ua.pdf (дата звернення: 19.01.2026).

29. Постанова колегії суддів Третьої судової палати ККС ВС від 12.06.2024 у справі № 569/1908/23. URL: https://reyestr.court.gov.ua/Review/119741340 (дата звернення: 19.01.2026).

30. Протокол Берклі з ведення розслідування 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; Женева: Центр із прав людини Каліфорн. ун-ту, Берклі, Юрид. шк., ООН Упр. Верхов. комісара з прав людини, 2020. URL: https://www.law.berkeley.edu/wp-content/uploads/ 2022/03/ Berkeley-ProtocolUkrainian.pdf (дата звернення: 19.01.2026).

31. Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. … д-ра філос.: 081 – Право. Львів. держ. ун-т внутр. справ. Львів, 2021. 248 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/3747 (дата звернення: 19.01.2026).

32. Розпочато досудове розслідування за фактами, оприлюдненими журналістами Слідство.Інфо, щодо підпільної школи на території монастиря. *Офіс Генерального прокурора :* веб-сайт. 07.01.2026. URL: https://gp.gov.ua/ua/posts/rozpocato-dosudove-rozsliduvannya-za-faktami-oprilyudnenimi-zurnalistami-slidstvoinfo-shhodo-pidpilnoyi-skoli-na-teritoriyi-monastirya

33. Розслідування колаборaційної діяльності: практ. посібник/ Є.О. Письменський, С.В.Головкін, А.В. Коваленко, В.В. Коваленко. Київ : ВД Дакор, 2024. 260 с.

34. Романюк А. Метод «гнилого оселедця»: хто і навіщо атакує журналістів. *Детектор медіа :* веб-сайт. 16.01.2025. URL: https://detector.media/blogs/article/221791/2024-01-16-metod-gnylogo-oseledtsya-khto-i-navishcho-atakuie-zhurnalistiv/

35. Скрипник А. В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2022. 408 с. DOI: https://doi.org/ 10.31359/ 9789669982940

36. Слінько Д. С, Слінько С. В., Стратонов В. М. Критерії процесуальної самостійності слідчого. *Наше право №1, 2023. С.35-41* http://nashe-pravo.unesco-socio.in.ua/wp-content/uploads/archive/NP-2023-1/NP-2023-1_044. pdf

37. Столітній А. В. Електронне кримінальне провадження на досудовому розслідуванні : дис. … д-ра юрид. наук: 12.00.2009. МВС України. Дніпропетров. держ. ун-т внутр. справ. Дніпро, 2018. 648 с. URL: https://dduvs.edu.ua/wpcontent/uploads/files/Structure/science/rada/dissertations/20/3.pdf

38. Стратонов В.М. Актуальні проблеми кримінального процесуального законодавства України в період воєнного стану. *Науковий вісник Херсонського державного університету. Серія: «Юридичні науки»* Випуск 4. 2025. С. 35-40. DOI https://doi.org/10.32999/ksu2307-8049/2025-4-6 (дата звернення: 19.01.2026).

39. Стратонов В.М. Повноваження слідчого судді у кримінальному провадженні. *Криміналістика і судова експертиза:* міжвідом. наук.-метод. зб. / Київський НДІ судових експертиз; редкол.: Д. В. Журавльов (голов. ред.), О. Г. Рувін (заст. голов. ред.) та ін. Київ : Видавництво Ліра-К, 2021. Вип. 66. С. 264-272 (дата звернення: 19.01.2026).

40. Стратонов В.М. Дзюрбель А.Д. Використання штучного інтелекту та інформаційних можливостей у створенні профіля злочинця. *Науковий вісник Херсонського державного університету. Серія: «Юридичні науки»* Випуск 5. 2024. Гельветика, 2024. С. 21-27. DOI: https://doi.org/10.32999/ksu2307-8049/2024-5-4 (дата звернення: 19.01.2026).

41. Стратонов В.М. Використання цифрових технологій у виявленні та документуванні фактів експлуатації людини під час збройних: доказова база в міжнародних судах. *Вчені записки ТНУ імені В.І. Вернадского. Серія: юридичні науки* Том 36 (75) № 1. 2025. С. 173-178. DOI https://doi.org/10.32782/TNU-2707-0581/2025.1/28 30.pdf (дата звернення: 19.01.2026).

42. Стратонов В.М., Гончарова О.В. Відмова прокурора від підтримання державного обвинувачення – навчально-методичний посібник. Харків: Право, 2020. 134 с.

43. Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду. *Верховний Суд :* веб-сайт. 28.10.2021. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/ (дата звернення: 19.01.2026).

44. Суддя Верховного Суду Наталія Марчук розповіла про судову практику щодо оцінювання електронних доказів у кримінальному провадженні. *Судово-юридична газета* : веб-сайт. 05.02.2025. URL: https://sud.ua/uk/news/sud-info/322490-sudya-verkhovnogo-suda-natalya-marchuk-rasskazala-o-sudebnoy-praktike-po-otsenke-elektronnykh-dokazatelstv-v-ugolovnom-proizvodstve (дата звернення: 19.01.2026).

45. Трикутник перевірки інформації в OSINT: як відрізнити факт від маніпуляції. *InsightOps :* веб-сайт. 26.08.2025. URL: https://insightops.com.ua/2025/08/26/%D1%82%D1%80%D0%B8%D0%BA%D1%83%D1%82%D0%BD%D0%B8%D0%BA%D0%BF%D0%B5%D1%80%D0%B5%D0%B2%D1%96%D1%80%D0%BA%D0%B8%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97-%D0%B2-osint-%D1%8F%D0%BA/ (дата звернення: 19.01.2026).

46. Ухвала Печерського районного суду м. Києва від 17.03.2016 року у справі № 757/12089/16-к. URL: http://reyestr.court.gov.ua/Review/56950544

47. Фоміна Т.Г., Рачинський О.О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник ХНУВС.* 2023. № 3(102). С. 207–220. DOI: https://doi.org/10.32631/v.2023.3.43 (дата звернення: 19.01.2026).

48. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція.* 2013. Вип. 5. С. 256–260. URL: http://nbuv. gov.ua/UJRN/ Nvmgu_jur_2013_5_58 (дата звернення: 19.01.2026).

49. Цивільний процесуальний кодекс України: Закон України від 18.03.2004 №1618-IV (зі змін. і доп.). URL: https://zakon.rada.gov.ua/laws/show/1618-15?find=1&text=електронні+#w1_11 (дата звернення: 19.01.2026).

Information about the authors:
Stratonov Vasyl Mykolaiovych,
Doctor of Law, Associate Professor, honored lawyer of Ukraine,
Professor of the Department of National, International Law and Law Enforcement Kherson State University,
27, Universytetska st., Kherson, 73035, Ukraine

Basysta Iryna Volodymyrivna,
Doctor of Legal Sciences, Professor,
Member of the Academic Advisory Council under the Supreme Court,
Professor at the Department of Law and Public Administration
King Danylo University
35, Y. Konovaltsia st., Ivano-Frankivsk, 76018, Ukraine

Hutnyk Alina,
Doctor of Philosophy in Law
10, Tykhoho Str., Kalush, 77300, Ukraine