DOI: 10.33498/louu-2025-09-060

III. Сучасні виклики та напрями розвитку кримінального процесуального законодавства України

Микола Погорецький

доктор юридичних наук, професор,
член-кореспондент НАПрН України,
заслужений діяч науки і техніки України,
професор кафедри кримінального процесу та криміналістики
Навчально-наукового інституту права,
проректор з науково-педагогічної роботи
Київського національного університету імені Тараса Шевченка
(Київ, Україна)
ORCID ID: https://orcid.org/0000-0003-0936-0929
mykola.pohoretskyi@knu.ua

УДК 343.13:343.98:342.7:004(477)

ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ В ЦИФРОВОМУ ДОКАЗУВАННІ ЯК УМОВА РЕАЛІЗАЦІЇ ПРИНЦИПУ ВЕРХОВЕНСТВА ПРАВА ТА ПОСТАНОВЛЕННЯ СПРАВЕДЛИВОГО ВИРОКУ

Анотація. Стаття присвячена комплексному аналізу забезпечення прав людини в цифровому доказуванні як ключової умови реалізації принципу верховенства права та постановлення справедливого вироку. У дослідженні підкреслюється, що цифрове доказування, як новий феномен доказового права, формує основу сучасного правосуддя, у якому технологічні можливості мають поєднуватися з непорушними процесуальними гарантіями людини. Розкрито поняття, ознаки та правову природу цифрового доказу, визначено його місце у структурі кримінального процесуального доказування та взаємозв'язок із принципами законності, пропорційності, змагальності сторін і справедливості. Особливу увагу приділено забезпеченню прав особи на приватність, захист персональних даних і ефективний судовий контроль при збиранні, перевірці та оцінці цифрових доказів.

Доведено, що якість цифрового доказування визначає реальність гарантій верховенства права, оскільки саме дотримання процесуальної форми, автентичності та цілісності електронних даних забезпечує справедливий вирок і довіру до правосуддя. У роботі проаналізовано міжнародно-правові стандарти, які формують аксіологічне підґрунтя цифрового доказування: стандарти Берклійського протоколу з цифрових розслідувань відкритих джерел, настанови Європейської мережі інститутів судової експертизи (ENFSI) щодо належної практики цифрової криміналістики, положення Конвенції про захист прав людини і основоположних свобод та прецеденти Європейського суду з прав людини *(Big Brother Watch and Others v. the UK, Roman Zakharov v. Russia, Glukhin v. Russia)*. Показано, що ці документи утворюють міжнародну модель забезпечення балансу між ефективністю правосуддя та дотриманням прав людини в цифровому середовищі.

Здійснено критичний аналіз чинного Кримінального процесуального кодексу України в аспекті регламентації цифрових доказів, виокремлено прогалини в процесуальній формі, пов'язані з відсутністю законодавчої дефініції "цифрового доказу" та механізмів фіксації ланцюга збереження даних. Запропоновано напрями вдосконалення кримінального процесуального законодавства, спрямовані на посилення процесуальних гарантій і забезпечення реального судового контролю за втручанням у цифрову приватність.

Обґрунтовано, що цифрове доказування має розвиватися як етична, правова й технологічна система, у якій пріоритетом є захист прав людини, дотримання верховенства права та забезпечення справедливого судового розгляду.

Ключові слова: цифрове доказування; права людини; верховенство права; справедливий суд; цифрова криміналістика; доказове право; досудове розслідування; ланцюг збереження; ЄСПЛ; ENFSI.

Цифровізація кримінального судочинства суттєво трансформує уявлення про доказування як про ядро процесуальної діяльності. Вона відкриває нові можливості для виявлення, фіксації та перевірки інформації про події злочину, але водночас створює серйозні виклики для гарантій прав людини, які становлять сутність принципу верховенства права. Цифрове доказування – це не лише технологічний феномен, а й категорія доказового права, у межах якої мають бути забезпечені такі базові цінності, як справедливий суд, змагальність сторін, презумпція невинуватості та право на повагу до приватного життя[1].

Поява цифрових доказів – результат розвитку інформаційних технологій, глобальних комунікаційних мереж та штучного інтелекту. Вони потребують нового підходу до процесуальної легалізації фактичних даних, які фіксуються в електронному вигляді, зберігаються у цифрових середовищах і можуть змінюватися без фізичних слідів втручання[2]. Питання автентичності, достовірності та допустимості цифрових доказів безпосередньо пов'язані з судовим контролем і справедливістю вироку.

Верховенство права в цьому контексті набуває особливого значення: воно виступає не декларацією, а критерієм допустимого втручання держави в цифрову приватність особи. Кожен етап цифрового доказування – від збирання до оцінки – має здійснюватися з дотриманням принципів законності, пропорційності та процесуальної справедливості[3].

Метою дослідження є комплексне дослідження механізмів забезпечення прав людини в цифровому доказуванні як інструменту реалізації принципу верховенства права та постановлення справедливого вироку. Основними завданнями є: з'ясування поняття й ознак цифрового доказу; аналіз впливу цифрових технологій на права людини та принцип змагальності; дослідження міжнародних стандартів цифрової криміналістики; формулювання пропозицій щодо вдосконалення національного кримінального процесуального законодавства.

Актуальність теми зумовлена тим, що в Україні досі не передбачена законодавча дефініція "цифровий доказ", а правові гарантії його використання залишаються фрагментарними. Цифрові сліди, метадані, записи з камер

[1] М Погорецький, 'Верховенство права у кримінальному процесуальному доказуванні: методологія та практика застосування' [2025] 32(3) Вісник Національної академії правових наук України 275–299.

[2] Best Practice Manuals and Forensic Guidelines (ENFSI) <https://enfsi.eu/documents/best-practice-manuals> (accessed 27.09.2025).

[3] Big Brother Watch and Others v. the United Kingdom. App 58170/13. European Court of Human Rights. Judgment. 25 May 2021 <https://hudoc.echr.coe.int/eng?i=001-210077> (accessed 27.09.2025).

спостереження, телекомунікаційні логи, OSINT-матеріали – усе це може мати ключове доказове значення, але без належного процесуального забезпечення є ризик того, що такі відомості можуть бути визнані недопустимими доказами в суді.

З огляду на зазначене цифрове доказування стає не лише технічною, а й аксіологічною проблемою, оскільки його якість визначає рівень захисту прав людини, ефективність судового контролю та довіру до правосуддя.

Теоретико-правові засади цифрового доказування. Цифрове доказування є одним із найдинамічніших і найвагоміших напрямів сучасного розвитку кримінального процесуального права. Його сутність полягає в збиранні, перевірці, оцінці та використанні відомостей, зафіксованих у цифровій формі, з метою встановлення обставин кримінального правопорушення. Водночас цифрова природа таких даних зумовлює нові вимоги до процесуальної форми, автентичності, ланцюга збереження *(chain of custody)* та перевірюваності джерел.

Традиційно в теорії доказ розглядається як єдність фактичних даних і процесуальної форми їх одержання[4]. Однак поява цифрових слідів – файлів, логів, хеш-ідентифікаторів, мережевих записів – створює гносеологічно інший рівень: дані можуть існувати без матеріального носія, а їхній зміст часто є результатом алгоритмічної обробки. Отже, зміст доказу розширюється, а класична категорія "джерело" набуває інформаційно-технічного виміру.

Під цифровим доказом доцільно розуміти зафіксовані у цифровій формі відомості про факти, що мають значення для кримінального провадження, які можуть бути сприйняті, перевірені та оцінені відповідно до процесуальних правил. Його юридична природа визначається не технічним способом існування інформації, а процесуальними гарантіями її достовірності[5].

Сучасна доктрина розглядає цифрове доказування як частину ширшої категорії – *digital forensics* (цифрової криміналістики), тобто сукупності наукових і технічних методів ідентифікації, збереження, аналізу й представлення електронних даних[6]. Такі методи охоплюють роботу з інформаційними системами, мобільними пристроями, хмарними сервісами, блокчейн-мережами, OSINT-джерелами. Їхня процесуальна легалізація потребує нормативного закріплення критеріїв допустимості, співмірності та прозорості.

[4] М Погорецький, 'Нова концепція кримінального процесуального доказування' [2015] 3 Вісник кримінального судочинства України 63–79; М Погорецький, 'Теорія доказів – методологічна основа оперативно-розшукового документування організованої злочинної діяльності' [2010] 22 Боротьба з організованою злочинністю і корупцією (теорія і практика) 175–185.

[5] М Погорецький, 'Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів (проблемні питання)' [2023] 3–4 Вісник кримінального судочинства 84–102 https://doi.org/10.17721/2413-5372.2023.3-4/84-102; М Погорецький, 'Цифрові технології та докази у розслідуванні злочинів проти основ національної безпеки України: процесуальні проблеми та європейські стандарти' [2025] 5(3) Аналітично-порівняльне правознавство 239–256; М Погорецький, 'Штучний інтелект у доказуванні в досудовому та судовому провадженнях: доктринальні засади і практика застосування' [2025] 91(4) Науковий вісник Ужгородського національного університету. Серія Право 398–418.

[6] Best Practice Manuals and Forensic Guidelines (n 2).

Особливістю цифрових доказів є їхня відтворюваність *(reproducibility):* достовірність цифрових даних має підтверджуватись можливістю незалежного відтворення процедури їх одержання й перевірки. Саме тому в міжнародній практиці утвердилися такі стандарти, як ведення *audit trail* (аудиторного ланцюга), хеш-підпису та криптографічної фіксації доказів[7].

У контексті українського процесуального права ці стандарти мають бути інтегровані в структуру процесуальної форми як умова допустимості.

У гносеологічній площині цифрове доказування зберігає усі риси класичного процесу доказування – пізнання, логічну верифікацію, оцінку доказів за внутрішнім переконанням суду. Проте джерела пізнання змінюються: замість матеріальних об'єктів дедалі частіше використовуються цифрові відображення, які не мають фізичних ознак. Відтак роль процесуальних гарантій значно зростає, адже саме вони компенсують нематеріальний характер доказового об'єкта.

У цьому аспекті цифрове доказування постає як новий рівень розвитку теорії доказів, що поєднує елементи інформаційного права, криміналістики та філософії процесуального пізнання. Його ключова особливість – потреба в балансі між ефективністю збирання доказів і дотриманням прав людини. Як слушно зазначає Європейський суд з прав людини (далі – ЄСПЛ), навіть у сфері національної безпеки держава не може виходити за межі необхідного втручання у приватність і комунікаційну свободу особи[8].

Отже, теоретичні засади цифрового доказування повинні базуватися на таких принципах: *законність* – цифрові дані можуть визнаватися доказами лише за умови їх одержання у спосіб, визначений законом; *автентичність* – має бути підтверджено незмінність цифрової інформації з моменту її фіксації; прозорість – методика збирання й аналізу даних повинна бути відтворюваною та підлягати експертній перевірці; *пропорційність* – втручання у цифрову приватність особи допускається лише в межах, необхідних для досягнення легітимної мети кримінального провадження; *справедливість* – цифрове доказування має забезпечувати рівність сторін і не створювати технологічної переваги держави над захистом.

Отже, *цифрове доказування* є не просто елементом сучасної процесуальної практики, а системотвірним чинником оновлення всієї теорії доказів у кримінальному процесі. Його розвиток має здійснюватися з урахуванням не лише технічних, а насамперед правових та етичних вимог, які гарантують реалізацію принципу верховенства права.

Верховенство права та судова справедливість у контексті цифрових доказів. Принцип верховенства права в кримінальному процесі має універ-

[7] Guidelines on Mobile Device Forensics, NIST SP 800-101 Rev. 1 (R Ayers, S Brothers, W Jansen, National Institute of Standards and Technology, U.S. Department of Commerce, 2014) https://doi.org/10.6028/NIST.SP.800-101r1.

[8] Roman Zakharov v. Russia. App 47143/06. European Court of Human Rights. Judgment. 4 December 2015 <https://hudoc.echr.coe.int/eng?i=001-159324> (accessed 27.09.2025).

сальний характер і є водночас критерієм легітимності державного втручання у права людини. Його реалізація в умовах цифровізації доказування потребує оновлення процесуальної парадигми – від формальної законності до змістової справедливості. Верховенство права в цьому аспекті визначає не лише законність дій сторін, а й якість процедур, що гарантують особі можливість ефективного захисту в цифровому середовищі[9].

З огляду на зростання ролі електронних доказів, цифрових слідів і даних, отриманих із телекомунікаційних систем, питання забезпечення прав людини набуває ключового значення. Судова практика ЄСПЛ сформувала низку критеріїв, які конкретизують вимогу верховенства права у сфері цифрового доказування. Зокрема, Суд наголошує на необхідності законності втручання, наявності ефективних гарантій проти зловживань, пропорційності обмежень і можливості незалежного судового контролю[10].

У справі *Roman Zakharov v. Russia* ЄСПЛ визначив, що будь-яка форма прихованого контролю за електронними комунікаціями має містити процесуальні запобіжники, які реально унеможливлюють свавільне втручання держави у приватне життя[11]. Аналогічна позиція викладена у рішенні *Big Brother Watch and Others v. the United Kingdom,* де Суд наголосив, що системне збирання та зберігання цифрових даних без належних процесуальних гарантій порушує принцип справедливого балансу між національною безпекою і правами людини[12].

Верховенство права у цифровому доказуванні означає, що кожен доказ має бути здобутий справедливим способом, із дотриманням процесуальних гарантій. Це передбачає не лише формальне дотримання закону, а й забезпечення реальної можливості сторони захисту оспорювати джерело, спосіб отримання та достовірність цифрових матеріалів. Без цього неможливо говорити про справедливий вирок, який є логічним завершенням дії принципу верховенства права.

Справедливість судового рішення не може бути забезпечена без мотивованої оцінки доказів у контексті їхньої придатності, допустимості, достовірності та достатності, а також без можливості ефективного судового контролю за дотриманням прав особи під час збирання доказів[13]. У цифровому просторі це означає, що суд має перевіряти не лише фактичні дані, а й технічні метадані, алгоритмічні процедури, програмні засоби, за допомогою яких отримано цифровий слід.

Верховенство права вимагає від суду мотивованого й відкритого тлумачення доказів – особливо тих, що створені або оброблені за допомогою тех-

[9] Погорецький (н 1) 275–299.
[10] Guidelines on Mobile Device Forensics (n 7).
[11] Roman Zakharov v. Russia (n 8).
[12] Big Brother Watch and Others v. the United Kingdom (n 3).
[13] М Погорецький, 'Судовий контроль у забезпеченні справедливого та допустимого доказування в кримінальному процесі України' [2025] 4(3) Аналітично-порівняльне правознавство 269–279 https://doi.org/10.24144/2788-6018.2025.04.3.40.

нологій штучного інтелекту. Якщо цифрове джерело не піддається людському розумінню через "алгоритмічну непрозорість" *(black box problem),* то використання таких даних без можливості перевірки суперечить як принципу верховенства права, так і вимозі справедливого суду[14].

Принцип справедливості у кримінальному процесі виявляється через збалансованість інтересів сторін і захист фундаментальних прав обвинуваченого. Саме тому цифрові технології мають використовуватися не як інструмент підміни доказування технічними засобами, а як допоміжний механізм, який посилює процесуальну істину без порушення прав людини.

У цьому контексті справедливий вирок є не лише результатом аналізу цифрових доказів, а й індикатором того, наскільки держава забезпечує рівність сторін, прозорість судового розгляду та публічне обґрунтування доказового рішення. Отже, верховенство права й справедливість формують єдиний правовий стандарт, що перетворює цифрове доказування на критерій легітимності правосуддя в епоху технологій.

Гарантії прав людини у цифровому доказуванні. Забезпечення прав людини в умовах цифровізації кримінального процесу є ключовою умовою реалізації принципу верховенства права. У цифровому доказуванні, де фактичні дані дедалі частіше мають електронну природу, традиційні механізми процесуальних гарантій мають бути переглянуті з урахуванням технологічних ризиків і нових форм втручання у приватність особи[15].

Передусім право на повагу до приватного життя, закріплене у ст. 8 Європейської конвенції з прав людини[16], охоплює захист електронних комунікацій, персональних даних, метаданих і цифрових профілів особи. Судова практика ЄСПЛ послідовно наголошує, що навіть збирання інформації без фактичного її використання може становити втручання у приватність, якщо не супроводжується чіткими процесуальними гарантіями[17].

У рішенні *Big Brother Watch and Others v. the United Kingdom* Суд сформулював вимоги до законності цифрового нагляду: наявність правової підстави, чітких меж дискреції, незалежного контролю, збереження даних лише протягом необхідного строку та надання особі засобів оскарження[18]. Ці критерії мають бути застосовними і до процесу цифрового доказування, адже інакше воно перетворюється на інструмент непропорційного втручання держави у сферу приватного життя.

[14] K Ligeti, M Hackenbruch, F Albrecht, A Monsalve Cuéllar et al., 'The Advent of AI: Reshaping Criminal Procedure' (University of Luxembourg, Faculty of Law, Economics and Finance, 2024) <https://aiandcriminaljustice.uni.lu/2024/11/06/the-advent-of-ai-reshaping-criminal-procedure> (accessed 27.09.2025).

[15] Погорецький (н 1) 275–299.

[16] Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини) <https://zakon.rada.gov.ua/laws/show/995_004#Text> (дата звернення 27.09.2025).

[17] Klass and Others v. Germany. App 5029/71. European Court of Human Rights. Judgment. 6 September 1978 <https://hudoc.echr.coe.int/eng?i=001-57510> (accessed 27.09.2025).

[18] Big Brother Watch and Others v. the United Kingdom (n 3).

В українському кримінальному процесі гарантії прав людини у сфері цифрових доказів залишаються недостатньо визначеними. Законодавство не містить окремої статті, що регламентувала б порядок збирання, перевірки та зберігання цифрових даних, хоча їх використання стало системним явищем у слідчій і судовій практиці. Відсутність процесуального визначення понять "цифровий доказ", "метадані", "електронна слідова інформація" створює ризики порушення права на захист та підстави для визнання доказів недопустимими[19].

Належна *гарантія прав особи* вимагає, щоб усі дії зі збору та аналізу цифрової інформації здійснювалися з дотриманням принципу законності, пропорційності й мінімізації втручання. У світовій практиці ці вимоги закріплені, зокрема, у *Berkeley Protocol on Digital Open Source Investigations* (2022), який встановлює стандарти верифікації цифрових матеріалів, визначає критерії достовірності відкритих джерел і фіксації ланцюга збереження доказів[20].

Забезпечення *автентичності* цифрових даних – ще одна фундаментальна гарантія. Вона передбачає документування кожного етапу роботи з електронними носіями – від вилучення до дослідження, з обов'язковим зазначенням технічних параметрів (час, алгоритм хешування, формат файлів). Згідно з настановами Європейської мережі інститутів судової експертизи (ENFSI) 2023 р. такі дії мають оформлюватися протоколами з унікальними ідентифікаторами, що уможливлює відтворити ланцюг збереження та довести незмінність об'єкта[21].

Особливе місце в системі гарантій належить *судовому контролю,* який є інструментом забезпечення балансу між інтересами слідства та правами особи. Суддя має оцінювати не лише зміст цифрового доказу, а й дотримання технологічних процедур його одержання. Судовий контроль у сфері цифрового доказування має набувати *ex ante* та *ex post* характеру – тобто здійснюватися як на етапі дозволу на втручання, так і на етапі перевірки законності здобутих матеріалів.

У змагальному кримінальному процесі захисник є суб'єктом доказування[22]. Тож важливою процесуальною гарантією є також *участь захисника* в оцінці цифрових доказів. Захисник повинен мати право ознайомлення з

[19] Погорецький, 'Цифрові технології та докази у розслідуванні злочинів…' (н 5) 239–256.

[20] 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 (OHCHR, University of California, Geneva–Berkeley 2022) <https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf> (accessed 27.09.2025).

[21] Best Practice Manuals and Forensic Guidelines (n 2).

[22] М Погорецький, 'Захисник – суб'єкт доказування на досудовому провадженні за чинним КПК України: проблемні питання', *Актуальні питання державотворення в Україні: матеріали міжнародної науково-практичної конференції (м. Київ, 23 травня 2014 р.)* (Прінт-Сервіс 2014) 480–482; О Старенький, *Кримінальні процесуальні гарантії захисника як суб'єкта доказування у досудовому розслідуванні: теорія та практика* (Алерта 2016); М Погорецький, Д Сергєєва, 'Тактика захисника: поняття, зміст та місце в системі криміналістичної тактики' [2016] 2 Вісник кримінального судочинства 113–123.

алгоритмами збору, копіювання, хешування й зберігання цифрової інформації, а також право ініціювати експертне дослідження програмного середовища чи електронного пристрою. Реалізація принципу "рівності сторін" у цифровому середовищі потребує технічної симетрії – доступу захисту до цифрових слідів і відповідних інструментів перевірки[23].

Водночас ефективність таких гарантій залежить від процесуального закріплення стандартів допустимості цифрових доказів. Доцільно, щоб у Кримінальному процесуальному кодексі України[24] (далі – КПК України) було передбачено положення, яке прямо визначає, що цифрові дані визнаються допустимими лише за умови забезпечення їхньої автентичності, цілісності, надійного збереження та дотримання прав учасників процесу.

Отже, гарантії прав людини у цифровому доказуванні виступають системою матеріальних і процесуальних механізмів, які забезпечують справедливість і достовірність результатів доказового процесу. Їх дотримання є передумовою не лише законності зібраних даних, а й легітимності судового рішення як втілення принципу верховенства права.

Міжнародні стандарти цифрової криміналістики та доказування. Міжнародна спільнота виробила низку технічних і процесуальних стандартів, що регулюють роботу з цифровими доказами, спрямованих на уніфікацію вимог до достовірності, автентичності й допустимості електронних даних. Ці стандарти є невід'ємною складовою глобальної системи захисту прав людини, адже визначають баланс між ефективністю правосуддя та гарантіями приватності[25].

Одним із ключових документів є *Берклійський протокол з цифрових розслідувань відкритих джерел (Berkeley Protocol on Digital Open Source Investigations,* 2020), ухвалений Управлінням Верховного комісара ООН з прав людини (OHCHR) та Каліфорнійським університетом у Берклі. Протокол уперше кодифікував стандарти збору, збереження, аналізу та представлення цифрових матеріалів з відкритих джерел для використання у кримінальних провадженнях і міжнародних розслідуваннях. Він передбачає обов'язковість фіксації ланцюга збереження *(chain of custody)*, верифікації метаданих, збереження оригіналу даних у незміненому вигляді та документування всіх технічних дій із цифровими носіями. Особливу увагу Протокол приділяє *етичним аспектам цифрового доказування,* зокрема, захисту персональних даних, безпеці осіб, які надають інформацію, і достовірності візуальних матеріалів. Він прямо пов'язує якість доказу з повагою до прав

[23] М Погорецький, М Щирук, 'Участь захисника у доказуванні у справах про привласнення або розтрату майна службовою особою: проблемні питання теорії та практики' [2025] 3(71) Knowledge, Education, Law, Management 139–150 https://doi.org/10.51647/kelm.2025.3.20.

[24] Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (дата звернення 27.09.2025).

[25] Погорецький (н 1) 275–299.

людини – що повністю відповідає концепції верховенства права в судовому процесі[26].

У європейському просторі провідну роль відіграє *Європейська мережа інститутів судової експертизи (ENFSI),* яка розробляє *Настанови належної практики у цифровій криміналістиці* (Best Practice Manuals – Digital Forensics). У виданнях 2015–2022 рр. закріплено методику збирання та дослідження цифрових доказів, включно з аудіо-, відео- та мережевими даними, стандартизовано алгоритми створення дублікатів, контрольних хешів, перевірки програмних середовищ[27].

ENFSI наголошує, що цифрова криміналістика є не лише технічним, а й правовим процесом. Вона повинна забезпечувати *прозорість і відтворюваність* усіх операцій з даними, а результати аналізу мають бути обґрунтовані, документовані й придатні для незалежної перевірки[28]. Це положення співзвучне із доктриною допустимості доказів, виробленою ЄСПЛ, за якою будь-яке порушення процедурних гарантій ставить під сумнів справедливість судового розгляду[29].

Серед інших важливих міжнародних орієнтирів варто назвати *Керівництво NIST SP 800-101 (rev.1) "Guidelines on Mobile Device Forensics"*, ухвалене Національним інститутом стандартів і технологій США. Документ визначає принципи вилучення, збереження та аналізу інформації з мобільних пристроїв, підкреслюючи, що достовірність цифрових доказів можлива лише за умови документування кожної технічної дії й використання сертифікованого програмного забезпечення[30].

Важливу роль відіграють також міжнародні стандарти *ISO/IEC 27037:2012,* що встановлюють принципи "ідентифікації, збору, збереження та передання цифрових доказів" у межах кримінального процесу. Стандарти ISO наголошують на потребі дотримання ланцюга автентичності *(evidence integrity chain)* та підготовки спеціалістів із цифрової криміналістики, які мають відповідні технічні й правові компетенції[31].

У межах Європейського Союзу питання транскордонного отримання цифрових доказів врегульовано *Директивою 2014/41/ЄС про Європейський ордер на розслідування (ЕІО),* яка передбачає взаємне визнання доказів між державами – членами ЄС та встановлює гарантії прав особи, щодо якої здійснюються процесуальні дії. Ця директива визначає, що цифрові дані

[26] Berkeley Protocol on Digital Open Source Investigations (n 20).
[27] Best Practice Manuals and Forensic Guidelines (n 2).
[28] Best Practice Manuals and Forensic Guidelines (n 2).
[29] Jalloh v. Germany. App 54810/00. European Court of Human Rights. Judgment. 11 July 2006 <https://hudoc.echr.coe.int/eng?i=001-76307> (accessed 27.09.2025).
[30] Guidelines on Mobile Device Forensics (n 7).
[31] ISO/IEC 27037:2012. Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence <https://www.iso.org/standard/44381.html> (accessed 27.09.2025).

можуть бути використані як докази лише за умови дотримання принципу пропорційності та контролю суду[32].

У практиці ЄСПЛ цифрові стандарти безпосередньо інтегровані в оцінку справедливості процесу. Так, у справах *Glukhin v. Russia* (2024) та *Zakharov v. Russia* (2015) Суд визнав, що використання технологій розпізнавання обличчя чи перехоплення цифрових комунікацій без законного регулювання порушує право на приватність і принцип "якість закону"[33].

Отже, міжнародні стандарти цифрової криміналістики мають не лише технічне, а й аксіологічне значення. Вони встановлюють універсальні критерії достовірності та справедливості цифрових доказів, слугують орієнтиром для гармонізації національного законодавства України з європейським і міжнародним правом. Інтеграція цих стандартів у кримінальний процес України є необхідною умовою забезпечення прав людини, реалізації принципу верховенства права та постановлення справедливого вироку.

Пропозиції щодо вдосконалення національного законодавства. Розвиток цифрового доказування в Україні вимагає не лише науково-методологічного осмислення, а й законодавчого врегулювання. На сьогодні КПК України не містить визначення поняття *цифрового доказу*, що створює прогалини в правозастосуванні, зокрема, при оцінці автентичності електронних даних, фіксуванні ланцюга збереження та захисті прав сторін. Ця невизначеність призводить до різного тлумачення допустимості цифрових матеріалів у судовій практиці, що суперечить принципу правової визначеності як складової верховенства права[34].

Першим кроком має стати *нормативне закріплення поняття "цифровий доказ"* у ст. 84 КПК України. Доцільно доповнити її новою частиною такого змісту:

"Цифровими доказами є відомості, зафіксовані у цифровій (електронній) формі на будь-яких носіях, що містять інформацію про факти, обставини чи події, які мають значення для кримінального провадження, одержані та досліджені у порядку, визначеному цим Кодексом, із забезпеченням їх автентичності, цілісності та можливості перевірки."

Таке визначення узгоджуватиме українське законодавство з міжнародними актами, зокрема ISO/IEC 27037:2012 і *Берклійським протоколом з цифрових розслідувань відкритих джерел,* у яких наголошено на вимогах достовірності, відтворюваності та простежуваності джерел.

Друге – потребує *уточнення ст. 99 КПК України,* яка визначає порядок долучення документів до матеріалів справи. Доцільно передбачити, що електронні носії, на яких містяться цифрові докази, повинні зберігатися в

[32] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters <http://data.europa.eu/eli/dir/2014/41/oj> (accessed 27.09.2025).
[33] Glukhin v. Russia. App 11519/20. European Court of Human Rights. Judgment. 4 July 2023 <https://hudoc.echr.coe.int/eng?i=001-225655> (accessed 27.09.2025); Roman Zakharov v. Russia (n 8).
[34] Погорецький (н 1) 275–299.

спеціальних умовах із фіксацією цифрового відбитку (хеш-суми), а кожне копіювання має супроводжуватися службовим протоколом, який є невід'ємною частиною матеріалів кримінального провадження.

Третє – необхідно *ввести окрему статтю щодо автентичності цифрових доказів,* у якій встановити: обов'язок слідчого та прокурора забезпечити фіксацію ланцюга збереження *(chain of custody)*; право сторони захисту на доступ до копій цифрових носіїв і програмних засобів, якими здійснювалася обробка даних; обов'язок суду перевіряти цілісність і відтворюваність цифрового доказу під час оцінки його допустимості.

Четверте – доцільно закріпити процесуальні гарантії недоторканності цифрової приватності в розділі КПК України, який регулює тимчасовий доступ до речей і документів (статті 159–166). Необхідно доповнити норми положеннями про заборону загального чи невибіркового вилучення інформації з електронних систем, а також про обов'язковість знищення даних, які не стосуються предмета провадження. Це відповідає стандартам ЄСПЛ у справах *Zakharov v. Russia* та *Big Brother Watch and Others v. the UK,* що встановлюють вимогу мінімізації втручання в особисте життя.

П'яте – варто *створити національний центр цифрової криміналістики,* уповноважений розробляти методики і стандарти роботи з цифровими доказами, проводити сертифікацію експертного програмного забезпечення та здійснювати міжвідомчий контроль за дотриманням вимог до ланцюга збереження даних. Такий центр міг би функціонувати при Міністерстві юстиції України в координації з Офісом Генерального прокурора, Службою безпеки України, Державним бюро розслідування та Національною поліцією.

Шосте – у межах професійної підготовки слідчих, прокурорів і суддів слід передбачити *обов'язкове навчання з цифрової криміналістики та прав людини у цифровому середовищі.* Згідно з рекомендаціями Ради Європи забезпечення цифрової компетентності юристів є необхідною умовою ефективного правосуддя в епоху технологій[35].

Сьоме – слід удосконалити *судову експертизу цифрових даних,* зокрема, шляхом унормування поняття "цифрова криміналістична експертиза", встановлення вимог до звітності експерта та процесуального статусу електронного висновку. Зазначене уможливить усунути колізії між положеннями КПК України та Закону України "Про судову експертизу"[36].

І, нарешті, варто забезпечити *узгодженість між кримінальним процесом і законодавством про кібербезпеку.* Закон України "Про основні засади забезпечення кібербезпеки України"[37] має бути доповнений розділом про вико-

[35] European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment, adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3-4 December 2018) <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> (accessed 27.09.2025).

[36] Guidelines on Mobile Device Forensics (n 7); Про судову експертизу: Закон України від 25 лютого 1994 року № 4038-XII <https://zakon.rada.gov.ua/laws/show/4038-12> (дата звернення 27.09.2025).

[37] Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення 27.09.2025).

ристання цифрових доказів у кримінальному провадженні, що гарантуватиме їх правову легітимність і захист персональних даних.

Реалізація цих пропозицій створить системну основу для формування цілісної моделі цифрового доказування в Україні – такої, що узгоджується з міжнародними стандартами, гарантує права людини та сприяє постановленню справедливих судових рішень. У цьому контексті справедливий вирок у цифрову епоху має оцінюватися не лише за змістом судового рішення чи логікою мотивувальної частини, а насамперед за якістю всього доказового процесу, у межах якого були зібрані, перевірені, автентифіковані й оцінені цифрові дані. Його легітимність залежить від того, чи забезпечено на практиці дотримання фундаментальних прав людини – права на приватність, права на ефективний засіб юридичного захисту, права на захист і принципу змагальності сторін, а також права бути судимим виключно на підставі достовірних, перевірених і допустимих доказів. Якщо цифрові дані використовуються без належних гарантій автентичності, без документування ланцюга збереження або без реальної можливості їх оскаржити, то сам процес втрачає ознаки справедливості, а вирок – ознаки легітимності, незалежно від того, чи є по суті правильними висновки суду.

У цьому сенсі правильний вирок і справедливий вирок – не тотожні категорії: перший може бути формально обґрунтованим, проте другий існує лише за умови дотримання прав людини на всіх етапах цифрового доказування. Цифрові сліди, алгоритмічні інструменти й засоби обробки даних створюють новий рівень ризиків для приватності та процесуальної рівноваги, а тому потребують регулювання за стандартами пропорційності, необхідності, прозорості та обов'язкового судового контролю. Забезпечення прав людини в цифровому доказуванні є не технічною деталлю, а маркером цивілізованості правової системи, показником її реальної відданості верховенству права та готовності обмежувати державне втручання строгими процесуальними гарантіями.

Саме тому цифрове доказування виходить далеко за межі технічного аспекту: воно перетворює технологічний інструментарій на етичну, правову та гарантійну категорію, яка уособлює практичне втілення верховенства права. Забезпечення прав людини в цій сфері визначає не лише якість судового рішення, а й рівень довіри суспільства до судової влади, формує межі допустимого втручання держави у цифрову приватність і запобігає зловживанням, що можуть виникати в умовах широкого використання високих технологій. Отже, захист прав людини у цифровому доказуванні є ключем до справедливого вироку, справжнім критерієм правової державності та фундаментом сучасної моделі кримінальної юстиції, яка повинна відповідати викликам інформаційної епохи й міжнародним стандартам справедливого суду.

Висновки. Цифрове доказування утворює новий рівень розвитку національного доказового права, який поєднує класичну гносеологію пізнання з

технологічними можливостями інформаційного суспільства. Його сутність полягає не лише у зміні форми збирання доказів, а й у трансформації самої методології доказування, що потребує забезпечення прав людини в умовах використання високих технологій.

Принцип верховенства права є ключовим нормативним орієнтиром для цифрового доказування. Він визначає межі допустимого втручання держави у цифрову приватність особи, вимагає дотримання пропорційності, передбачуваності та наявності ефективних процесуальних гарантій. Верховенство права в цифровому середовищі реалізується через стандарти законності, справедливості, прозорості та рівності сторін.

Гарантії прав людини у цифровому доказуванні охоплюють не лише формальну заборону порушення приватності, а й забезпечення автентичності, цілісності та надійного збереження електронних даних. Вони передбачають право сторони захисту на технічний доступ до джерел цифрових доказів, право на оскарження способу їх отримання, а також обов'язок суду перевіряти ланцюг збереження та допустимість кожного цифрового матеріалу.

Міжнародні стандарти – Берклійський протокол (2020), Настанови ENFSI (2023–2025), ISO/IEC 27037:2012, Директива 2014/41/ЄС, а також практика ЄСПЛ – формують уніфіковану систему орієнтирів для цифрової криміналістики. Їх імплементація в українське процесуальне право забезпечить єдність критеріїв допустимості цифрових доказів, запровадить перевірювані процедури автентифікації та сприятиме реалізації принципу справедливого суду.

Удосконалення КПК України має здійснюватися шляхом: введення юридичного визначення поняття "цифровий доказ"; установлення процесуальних вимог до автентичності та ланцюга збереження; нормативного врегулювання судового контролю за цифровими доказами; закріплення гарантій участі сторони захисту в дослідженні цифрових матеріалів; створення національного центру цифрової криміналістики при Міністерстві юстиції України.

Справедливий вирок у цифрову епоху має оцінюватися не лише за змістом судового рішення, а й за якістю доказового процесу. Його легітимність визначається тим, наскільки цифрові дані, використані в суді, були зібрані й перевірені у спосіб, що забезпечує дотримання прав людини, змагальність сторін і прозорість процедур.

У підсумку, забезпечення прав людини у цифровому доказуванні – це не лише гарантія правосуддя в конкретному провадженні, а й показник цивілізованості правової системи. Воно перетворює технологічний інструментарій на етичну та правову категорію, втілюючи принцип верховенства права у практиці доказування та формуючи довіру суспільства до судової влади.

REFERENCES

Bibliography

Authored books

1. Starenkyi O, *Kryminalni protsesualni harantii zakhysnyka yak sub'iekta dokazuvannia u dosudovomu rozsliduvanni: teoriia ta praktyka* (Alerta 2016) (in Ukrainian).

Journal articles

2. Pohoretskyi M, 'Verkhovenstvo prava u kryminalnomu protsesualnomu dokazuvanni: metodolohiia ta praktyka zastosuvannia' [2025] 32(3) Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy 275–299 (in Ukrainian).
3. Pohoretskyi M, 'Zastosuvannia novitnikh tekhnolohii u rozsliduvanni ta dokazuvanni voiennykh zlochyniv (problemni pytannia)' [2023] 3–4 Visnyk kryminalnoho sudochynstva 84–102 https://doi.org/10.17721/2413-5372.2023.3-4/84-102 (in Ukrainian).
4. Pohoretskyi M, 'Nova kontseptsiia kryminalnoho protsesualnoho dokazuvannia' [2015] 3 Visnyk kryminalnoho sudochynstva Ukrainy 63–79 (in Ukrainian).
5. Pohoretskyi M, 'Sudovyi kontrol u zabezpechenni spravedlyvoho ta dopustymoho dokazuvannia v kryminalnomu protsesi Ukrainy' [2025] 4(3) Analitychno-porivnialne pravoznavstvo 269–279 https://doi.org/10.24144/2788-6018.2025.04.3.40 (in Ukrainian).
6. Pohoretskyi M, 'Teoriia dokaziv – metodolohichna osnova operatyvno-rozshukovoho dokumentuvannia orhanizovanoi zlochynnoi diialnosti' [2010] 22 Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka) 175–185 (in Ukrainian).
7. Pohoretskyi M, 'Tsyfrovi tekhnolohii ta dokazy u rozsliduvanni zlochyniv proty osnov natsionalnoi bezpeky Ukrainy: protsesualni problemy ta yevropeiski standarty' [2025] 5(3) Analitychno-porivnialne pravoznavstvo 239–256 (in Ukrainian).
8. Pohoretskyi M, 'Shtuchnyi intelekt u dokazuvanni v dosudovomu ta sudovomu provadzhenniakh: doktrynalni zasady i praktyka zastosuvannia' [2025] 91(4) Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia Pravo 398–418 (in Ukrainian).
9. Pohoretskyi M, Serhieieva D, 'Taktyka zakhysnyka: poniattia, zmist ta mistse v systemi kryminalistychnoi taktyky' [2016] 2 Visnyk kryminalnoho sudochynstva 113–123 (in Ukrainian).
10. Pohoretskyi M, Shchyruk M, 'Uchast zakhysnyka u dokazuvanni u spravakh pro pryvlasnennia abo roztratu maina sluzhbovoiu osoboiu: problemni pytannia teorii ta praktyky' [2025] 3(71) Knowledge, Education, Law, Management 139–150 https://doi.org/10.51647/kelm.2025.3.20 (in Ukrainian).

Conference papers

11. Pohoretskyi M, 'Zakhysnyk – sub'iekt dokazuvannia na dosudovomu provadzhenni za chynnym KPK Ukrainy: problemni pytannia', *Aktualni pytannia derzhavotvorennia v Ukraini: materialy mizhnarodnoi naukovo-praktychnoi konferentsii (m. Kyiv, 23 travnia 2014 r.)* (Print-Servis 2014) 480–482 (in Ukrainian).

Websites

12. 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 (OHCHR, University of California, Geneva–Berkeley 2022) <https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf> (accessed 27.09.2025).
13. Guidelines on Mobile Device Forensics, NIST SP 800-101 Rev. 1 (R Ayers, S Brothers, W Jansen, National Institute of Standards and Technology, U.S. Department of Commerce, 2014) https://doi.org/10.6028/NIST.SP.800-101r1.

14. Ligeti K, Hackenbruch M, Albrecht F, Monsalve Cuéllar A et al., 'The Advent of AI: Reshaping Criminal Procedure' (University of Luxembourg, Faculty of Law, Economics and Finance, 2024) <https://aiandcriminaljustice.uni.lu/2024/11/06/the-advent-of-ai-reshaping-criminal-procedure> (accessed 27.09.2025).

Mykola Pohoretskyi

ENSURING HUMAN RIGHTS IN DIGITAL EVIDENCE AS A CONDITION FOR THE IMPLEMENTATION OF THE RULE OF LAW AND THE DELIVERY OF A FAIR VERDICT

Abstract. The article provides a comprehensive analysis of ensuring human rights in digital evidence as a key condition for the implementation of the rule of law and the delivery of a fair verdict. The study emphasizes that digital evidence, as a new phenomenon of evidence law, forms the foundation of modern justice, in which technological capabilities must be combined with inviolable procedural guarantees of the individual. The article clarifies the concept, features, and legal nature of digital evidence, determines its place within the structure of criminal evidentiary proceedings, and examines its relationship with the principles of legality, proportionality, adversarial proceedings, and fairness. Particular attention is paid to safeguarding the right to privacy, personal data protection, and effective judicial control during the collection, verification, and assessment of digital evidence.

It is demonstrated that the quality of digital evidence determines the real effectiveness of the guarantees of the rule of law, as adherence to procedural form, authenticity, and integrity of electronic data ensures both a fair verdict and public confidence in the justice system. The article analyzes international legal standards that constitute the axiological foundation of digital evidence: the standards of the Berkeley Protocol on Digital Open Source Investigations, the guidelines of the European Network of Forensic Science Institutes (ENFSI) on proper practice in digital forensics, the provisions of the European Convention on Human Rights, and the case law of the European Court of Human Rights *(Big Brother Watch and Others v. the UK, Roman Zakharov v. Russia, Glukhin v. Russia)*. These documents are shown to form an international model for balancing the effectiveness of justice with the protection of human rights in the digital environment.

A critical analysis is conducted of the current Criminal Procedure Code of Ukraine regarding the regulation of digital evidence, identifying gaps in procedural form related to the absence of a legislative definition of "digital evidence" and mechanisms for documenting the chain of custody of electronic data. The article proposes directions for improving criminal procedure legislation aimed at strengthening procedural safeguards and ensuring effective judicial control over state interference in digital privacy.

It is substantiated that digital evidence must develop as an ethical, legal, and technological system in which the protection of human rights, adherence to the rule of law, and the guarantee of a fair trial are absolute priorities.

Keywords: digital evidence; human rights; rule of law; fair trial; digital forensics; evidentiary law; pre-trial investigation; chain of custody; ECHR; ENFSI.