

## КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 343.140.02

DOI <https://doi.org/10.32782/TNU-2707-0581/2025.4/21>

**Горєлова В. Ю.**

Таврійський національний університет імені В.І. Вернадського

**Горелкіна К. Г.**

Таврійський національний університет імені В.І. Вернадського

### АВТЕНТИЧНІСТЬ ЯК КРИТЕРІЙ ДОПУСТИМОСТІ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ: КОМПАРАТИВНИЙ АНАЛІЗ ТА НАПРЯМИ УДОСКОНАЛЕННЯ

*У статті здійснено ґрунтовне дослідження складного та багатогранного феномену використання цифрових доказів у кримінальному процесі України. Ця тема набуває критичної ваги та стратегічного значення в умовах всезростаючої цифровізації суспільства та прогресуючих загроз у сфері кіберзлочинності. Основна увага зосереджена на виявленні ключових юридичних, нормативних і процесуальних викликів, які виникають під час інтеграції електронних доказів у систему національного судочинства.*

*У статті проведено методологічний аналіз передумов і критеріїв забезпечення автентичності та допустимості цифрових джерел доказової інформації, які є визначальними чинниками їхньої юридичної значущості та здатності впливати на результативність кримінального провадження. Досліджено прогалини, суперечності й правові колізії в чинному законодавстві, що перешкоджають належному нормативному закріпленню процедур збирання, обробки, збереження та процесуального використання цифрових доказів.*

*Особливу увагу приділено глибокому порівняльному аналізу міжнародно-правових актів, зокрема положень Конвенції Ради Європи про кіберзлочинність, та практики впровадження електронних доказів у юрисдикціях зарубіжних держав. Аналіз досвіду країн Європейського Союзу, Великої Британії, Канади та Естонії дозволив виокремити ефективні моделі створення спеціалізованих підрозділів, розробки технічних протоколів фіксації та верифікації цифрових слідів.*

*За результатами дослідження, сформульовано комплекс системних рекомендацій, спрямованих на вдосконалення українського кримінального процесуального законодавства. Вони включають чітке законодавче визначення поняття цифрового доказу, створення нормативної класифікації його форм, запровадження уніфікованих процедур автентифікації та допустимості, а також інституціоналізацію спеціалізованої експертизи цифрових джерел. Результати дослідження становлять вагомий внесок у формування концептуально оновленої моделі цифрового судочинства в Україні.*

**Ключові слова:** цифрові докази, електронні докази, кримінальний процес, автентичність доказів, допустимість доказів, кіберзлочинність, судова експертиза, кібербезпека.

**Постановка проблеми.** В умовах стрімкої цифровізації всіх сфер суспільного життя та безперервного зростання обсягів кіберзлочинності, ефективність кримінального судочинства в Україні безпосередньо залежить від здатності правової системи адаптуватися до цих викликів. Однією

з найбільш гострих та актуальних проблем є використання цифрових доказів у кримінальному процесі. Незважаючи на їхню зростаючу роль у викритті злочинів, національне законодавство та правозастосовна практика стикаються зі значними труднощами щодо забезпечення автентичнос-

ті, допустимості, належної фіксації та зберігання електронної інформації. Ці недоліки, які проявляються, наприклад, у відсутності єдиних стандартів щодо скріншотів переписки або вилучення даних з хмарних сховищ без відповідних міжнародних процедур, ставлять під загрозу легітимність судових рішень та підривають довіру до системи правосуддя. Така ситуація вимагає негайного та комплексного наукового осмислення та пошуку шляхів їх подолання.

**Аналіз останніх досліджень і публікацій.** Питання використання цифрових доказів у кримінальному процесі України та суміжних правових проблематик були предметом активних наукових досліджень низки вітчизняних учених. Зокрема, у працях Гутник В. В. і Хитра О. Б. (2022) [1], Лисаченка С. В. (2021) [2], Скрипника Ю. С. (2022) [3], Шевчука В. Ю. (2020) [4], а також Лук'янчикова Є. Д. та співавторів (2020–2023) [5], Мельника О. Ю. (2022) [6], Музиченка О. В. і Карандась М. В. (2022) [7] були висвітлені теоретичні засади електронних доказів, їх класифікація, а також окремі аспекти процесуального порядку збирання, оцінки та використання.

Попри значний внесок цих авторів у розробку окремих елементів доказування цифровою інформацією, слід зазначити, що комплексний аналіз проблеми забезпечення автентичності та допустимості цифрових доказів у взаємозв'язку з міжнародно-правовими орієнтирами залишається недостатньо висвітленим. Наявні дослідження не завжди повною мірою охоплюють динаміку судової практики та прецедентів Європейського суду з прав людини, а також не інтегрують у достатній мірі положення Конвенції Ради Європи про кіберзлочинність [8]. До того ж, українська наукова література, попри свою цінність, часто відчуває нестачу глибокого порівняльного аналізу з європейськими та англійськими дослідженнями у сфері Digital Evidence and Electronic Signature Law, що є важливим для уніфікації підходів та розуміння міжнародних тенденцій [9; 10]. Це свідчить про наявність суттєвих прогалин у науковому обґрунтуванні, що вимагає подальшого поглибленого, системного та порівняльно-правового дослідження.

**Постановка завдання.** Метою цієї статті є проведення комплексного аналізу проблем, пов'язаних із використанням цифрових доказів у кримінальному процесі України. Ми акцентуємо увагу на критичних питаннях їхньої автентичності, допустимості та відповідності міжнародно-правовим орієнтирам, зокрема практиці Європейського суду з прав людини (ЄСПЛ) та положенням Конвенції

Ради Європи про кіберзлочинність (Будапештської конвенції). Дослідження спрямоване на виявлення та систематизацію наявних законодавчих прогалин і практичних недоліків, що перешкоджають ефективному застосуванню електронної інформації як джерела доказів. Кінцевим завданням є розробка науково обґрунтованих рекомендацій щодо вдосконалення національного кримінального процесуального законодавства та правозастосовної практики. Це має забезпечити гармонізацію із зазначеними міжнародними стандартами та підвищити ефективність кримінального судочинства в умовах інтенсивної цифровізації.

**Виклад основного матеріалу.** Поняття та правова природа цифрових доказів досі залишаються дискусійними у вітчизняному кримінальному процесуальному дискурсі. Нормативно-правова база України не містить легального визначення терміна «цифровий доказ», що об'єктивно ускладнює його ідентифікацію, належну фіксацію, процесуальне оформлення та подальшу оцінку в межах кримінального провадження. Така правова невизначеність спричиняє неоднозначність у кваліфікації відповідних об'єктів, обмежує ефективність використання цифрових джерел інформації та створює ризики для забезпечення належного рівня доказової діяльності сторін процесу.

Міжнародне співтовариство, зокрема в межах положень Будапештської конвенції про кіберзлочинність, підкреслює потребу у формалізації підходів до обігу цифрових слідів як доказів, беручи до уваги їхні унікальні властивості – нестабільність, вразливість до зовнішніх впливів, змінюваність та складність достовірної ідентифікації джерела походження. Ці характеристики вимагають від національного правозастосування вироблення особливих процесуальних стандартів, які б забезпечували автентичність цифрових доказів, зберігаючи баланс між інтересами правосуддя і правами учасників провадження. Таким чином, потреба в комплексному науково-практичному осмисленні правової природи цифрових доказів набуває особливої актуальності у зв'язку зі стрімкою цифровізацією суспільства та відповідними трансформаціями у сфері кримінального судочинства.

Сучасний розвиток інформаційних технологій, що невпинно інтегруються в усі сфери суспільного життя, зумовлює трансформацію кримінального процесу, актуалізуючи потребу в адаптації його інструментарію до нових реалій. Однією з найсуттєвіших та найбільш комплексних проблем, що постають перед правозастосовними органами в Україні, є відсутність чітких, уніфікованих

процесуальних стандартів фіксації, зберігання та подальшої передачі цифрових доказів [11]. Цей чинник істотно ускладнює ефективне використання електронної інформації у доказовій базі кримінальних проваджень.

Нерідко спостерігається ситуація, коли слідчі та інші уповноважені особи, попри значний прогрес у цифровізації, не володіють достатнім рівнем спеціалізованої технічної кваліфікації. Це значно ускладнює або навіть унеможлиблює коректну імплементацію цифрових доказів у процес, що безпосередньо призводить до порушення фундаментального принципу допустимості доказів [12]. Зазначені прогалини створюють ризики для процесуальної легітимності отриманих даних та їхньої подальшої юридичної сили.

На практиці зустрічаються численні випадки, що ілюструють системні недоліки в роботі з цифровими слідами. Зокрема, досить поширеним є надання суду скріншотів електронної переписки або окремих електронних листів без проведення належної технічної експертизи, яка могла б підтвердити їхню автентичність та цілісність [13]. Аналогічно, вилучення даних із хмарних сховищ нерідко здійснюється без дотримання встановлених вимог міжнародного співробітництва або без залучення до цього процесу відповідних провайдерів послуг, що може призвести до порушення суверенітету даних та міжнародно-правових норм. Окрему увагу слід звернути на відеозаписи, отримані з камер відеоспостереження, які часто надаються без супровідних метаданих. Відсутність такої критично важливої інформації, як час, дата, місце та обставини зйомки, фактично унеможлиблює ідентифікацію подій та верифікацію наданих матеріалів, ставлячи під сумнів їхню доказову цінність.

Перелічені вище обставини об'єктивно ставлять під сумнів процесуальну чистоту отримання цифрових доказів і несуть у собі значний ризик визнання їх недопустимими судом. Це, своєю чергою, може призвести до нівелювання зусиль правоохоронних органів та перешкоджати встановленню об'єктивної істини у кримінальному провадженні, підриваючи ефективність системи правосуддя загалом.

Логічним продовженням проблематики фіксації та зберігання цифрових доказів є питання забезпечення їхньої автентичності та допустимості в умовах чинної правової системи. Варто зазначити, що у Кримінальному процесуальному кодексі України [14] наразі відсутня деталізована та всеосяжна процедура верифікації електронних доказів. Цей нормативний вакуум створює значні перешкоди для ефективного застосування цифрових даних у судо-

вій практиці. Зокрема, законодавчо не визначено чіткого механізму підтвердження справжності цифрових даних, що залишає простір для різночитань та зловживань. Не менш критичною є неврегульованість питання щодо забезпечення цілісності інформації під час її передачі від джерела до суб'єктів доказування, що є фундаментальною вимогою для збереження доказової цінності. Крім того, на сьогодні в Україні не існує єдиного, загальноприйнятого стандарту для проведення цифрової експертизи, що призводить до фрагментації підходів та ускладнює уніфікацію судової практики.

Зазначені нормативні прогалини об'єктивно ускладнюють процес доведення достовірності джерела інформації, яка є основою для формування внутрішнього переконання суду. Це створює сприятливе підґрунтя для потенційних маніпуляцій з цифровими даними або навіть їхньої фальсифікації, що може суттєво спотворити результати судового розгляду. Аналіз сучасної судової практики свідчить про нерідкий формальний підхід до оцінки цифрових доказів [7]. Суди часто приймають або відхиляють такі докази без повного, ґрунтовного дослідження їхніх технічних характеристик, не враховуючи специфіку електронних носіїв та способів фіксації. Така практика, безумовно, суперечить вимогам справедливого судового розгляду та принципам всебічності, повноти й об'єктивності дослідження обставин кримінального провадження. Отже, відсутність належного правового регулювання та єдиних стандартів щодо автентичності та допустимості цифрових доказів залишається одним із ключових викликів у сучасній українській системі кримінальної юстиції, що вимагає невідкладного комплексного вирішення.

У контексті окреслених національних проблемних аспектів, особливого значення набувають міжнародно-правові орієнтири, зокрема прецедентна практика Європейського суду з прав людини (ЄСПЛ). У низці своїх знакових рішень, серед яких варто виокремити справи «Khan v. The United Kingdom» [15] та «Barbulescu v. Romania» [16], ЄСПЛ послідовно наголошує на імперативній вимозі, згідно з якою використання електронних доказів у кримінальному провадженні має неухильно відповідати принципу «належної правової процедури» (due process). Це комплексне положення охоплює декілька ключових аспектів, спрямованих на забезпечення справедливості та збалансованості судового розгляду.

Передусім, зазначений принцип передбачає, що сторона захисту повинна мати повноцінний та ефективний доступ до джерела цифрового дока-

зу, включаючи можливість його незалежного вивчення та аналізу. Крім того, має бути гарантована можливість оскарження способу його отримання, що дозволяє перевірити відповідність дій правоохоронних органів вимогам закону та захистити права підозрюваних/обвинувачених від можливих порушень. Важливою складовою є також вимога до самого суду: він зобов'язаний ретельно та всебічно перевірити умови збирання та цілісність доказу, особливо у випадках, коли йдеться про застосування оперативно-розшукових заходів або проведення негласних слідчих дій. Це стосується не лише первинного отримання, а й подальшого зберігання та передачі інформації, аби уникнути будь-яких несанкціонованих змін чи спотворень [17].

Україна як держава-учасниця Конвенції про захист прав людини і основоположних свобод [18] несе пряме зобов'язання імплементувати ці високі міжнародні стандарти у своє національне законодавство та правозастосовну практику. Однак, попри ратифікацію Конвенції та визнання юрисдикції ЄСПЛ, на практиці ці вимоги нерідко ігноруються

або тлумачаться вибірково, що створює значний дисонанс між проголошеними зобов'язаннями та їх реальним виконанням. Це підкреслює нагальну потребу в подальшій гармонізації національного кримінального процесуального законодавства та підвищенні правової свідомості учасників процесу щодо важливості дотримання міжнародних стандартів у роботі з цифровими доказами.

У процесі дослідження було виявлено низку системних проблем, пов'язаних із використанням цифрових доказів у кримінальному процесі України. Вони охоплюють як нормативно-правовий рівень, так і практичні аспекти їх збирання, зберігання, оцінки та судового застосування. Особливу увагу привертає неврегульованість питань автентичності й допустимості електронних доказів, відсутність чітких процесуальних стандартів, а також недостатній рівень інтеграції міжнародних правових орієнтирів у національну практику. Водночас аналіз судової практики та міжнародного досвіду дозволив сформулювати низку конструктивних пропозицій щодо вдосконалення відповідних механізмів.

Таблиця 1

| Категорія                      | Суть проблеми / характеристика                                 | Критичні виклики                                    | Запропоновані рішення / рекомендації                                   |
|--------------------------------|----------------------------------------------------------------|-----------------------------------------------------|------------------------------------------------------------------------|
| Нормативно-правове регулювання | Відсутність легального визначення цифрового доказу             | Неоднозначність тлумачення, правова невизначеність  | Внесення чіткого визначення до КПК, класифікація форм цифрових доказів |
| Процесуальні стандарти         | Відсутність уніфікованих процедур збирання, фіксації, передачі | Ризик фальсифікації, втрати доказової цінності      | Розробка уніфікованих протоколів і технічних стандартів                |
| Автентичність доказів          | Немає загального механізму верифікації цифрових джерел         | Неможливість встановити достовірність               | Запровадження процедур автентифікації, перевірки джерела               |
| Судова практика                | Формальний підхід до оцінки цифрових доказів                   | Ігнорування технічних аспектів і метаданих          | Обов'язковість аналізу умов збирання, технічної експертизи             |
| Технічна підготовка            | Недостатня кваліфікація слідчих і суддів                       | Некоректна імплементація доказів                    | Освітні програми та підвищення кваліфікації                            |
| Міжнародні стандарти           | Ігнорування практики ЄСПЛ, Будапештської конвенції             | Дисонанс між зобов'язаннями й практикою             | Гармонізація КПК з положеннями Конвенцій та рішень ЄСПЛ                |
| Експертиза цифрових доказів    | Відсутність спеціалізованої цифрової експертизи                | Фрагментація підходів, ненадійність результатів     | Інституалізація експертизи, впровадження єдиних методик                |
| Судовий контроль               | Відсутній контроль за ланцюгом зберігання даних                | Порушення принципів допустимості, втрата цілісності | Встановлення обов'язкових стандартів контролю ланцюга збереження       |
| Міжнародна практика            | Обмежене врахування досвіду інших країн (Канада, Естонія тощо) | Відсутність уніфікації, відставання від тенденцій   | Запозичення успішних моделей, створення спеціалізованих підрозділів    |
| Загальна оцінка ситуації       | Незбалансованість національної системи цифрового доказування   | Ризик недопустимості, втрата довіри до правосуддя   | Системна реформа: нормативна, інституційна, освітня                    |

З метою логічної узагальненості та зручності візуального сприйняття основні проблемні позиції, пов'язані з використанням цифрових доказів, їх ключові виклики та напрями вдосконалення систематизовано у Таблиці 1. Представлена інформація дозволяє чітко зіставити існуючі недоліки з відповідними пропозиціями реформування та може слугувати основою для подальших нормативно-правових і організаційних рішень.

Таблиця є концентрованим резюме аналізу поточної ситуації, викликів та необхідних напрямків удосконалення у сфері застосування цифрових доказів, що є надзвичайно корисним для розуміння суті проблеми та шляхів її вирішення.

**Висновки.** Проведений аналіз виразно засвідчує, що використання цифрових доказів у кримінальному процесі України наразі залишається вкрай неурегульованим і вразливим до численних зловживань. Системна відсутність уніфікованої, чітко визначеної та всеосяжної процедури збирання, зберігання та верифікації таких доказів, поряд із недостатнім та, на жаль, часто поверховим судовим контролем за процесом їхнього формування, неминуче призводить до порушення фундаментальних процесуальних гарантій учасників справи. Це, своєю чергою, створює значні ризики визнання вироків несправедливими та підриває довіру суспільства до правосуддя.

Для вирішення окреслених проблем, які мають критичне значення для ефективності та легітимності кримінального судочинства в цифрову епоху, вбачається необхідним вжити низку невідкладних і комплексних заходів. Зокрема, першочерговим завданням є розробка уніфікованого підзаконного акта або внесення ґрунтовних змін та доповнень до Кримінального процесуального кодексу Украї-

ни, які б детально регламентували обіг цифрових доказів на всіх стадіях кримінального провадження – від виявлення та вилучення до оцінки та використання. Таке нормативне оновлення має чітко визначити процесуальний статус, види, форми та методи роботи з електронними даними.

Окрім цього, вкрай важливо запровадити систему спеціалізованої цифрової експертизи, яка ґрунтувалася б на чітко визначених методиках, єдиних стандартах та протоколах, визнаних на міжнародному рівні. Це забезпечить об'єктивність, достовірність та відтворюваність результатів дослідження цифрових носіїв інформації. Паралельно з цим необхідно суттєво розширити та поглибити програми підготовки слідчих, прокурорів і суддів щодо технічних аспектів цифрових слідів, особливостей їхньої фіксації, аналізу та правової оцінки. Це дасть змогу підвищити їхню кваліфікацію та забезпечити компетентний підхід до роботи з електронними доказами.

Нарешті, безумовною вимогою є гармонізація українського законодавства з відповідними положеннями Європейської конвенції про захист прав людини та основоположних свобод, а також Конвенції Ради Європи про кіберзлочинність (Будапештської конвенції). Впровадження міжнародних стандартів дозволить не лише зміцнити правові позиції України на міжнародній арені, а й забезпечити дотримання прав людини в умовах стрімкого розвитку цифрових технологій.

Усунення означених прогалин є не просто техніко-юридичним викликом, а стратегічною необхідністю. Це є ключовим чинником для підвищення довіри до судочинства та забезпечення його ефективності в умовах безперервної цифрової трансформації правової системи України.

#### Список літератури:

1. Гутник В. В., Хитра О. Б. Електронні докази у кримінальному провадженні: теорія та практика: монографія. Львів, 2022. 240 с. URL: [https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/Гутник\\_Хитра\\_монографія\\_2022.pdf](https://dspace.lvduvs.edu.ua/bitstream/1234567890/4725/1/Гутник_Хитра_монографія_2022.pdf)
2. Лисаченко С. В. Цифрові докази в кримінальному провадженні: сучасний стан та перспективи. Одеса, 2021. 176 с.
3. Скрипник Ю. С. Електронні докази в системі доказування в кримінальному процесі. Київ, 2022. 190 с.
4. Шевчук В. Ю. Електронні докази та їх значення для кримінального провадження. Житомир, 2020. 148 с.
5. Лук'янчиков Є. Д., Лук'янчиков Б. Є., Микитенко О. Б. Співвідношення висновку експерта з висновком спеціаліста у кримінальних проступках. *UzhNU Jure Journal*. 2023. URL: <https://dspace.uzhnu.edu.ua/jspui/handle/lib/54621>
6. Мельник О. Ю. Проблеми оцінки цифрових доказів у кримінальному провадженні. *Право і суспільство*. 2022. № 1. С. 167–173.
7. Музиченко О. В., Карандась М. В. Електронні докази як джерела доказів у межах кримінального провадження: судова практика та нормативне регулювання. *Київський часопис права*. 2022. № 2. С. 76–81. URL: <https://kyivchasprava.kneu.in.ua/index.php/kyivchasprava/article/view/179>

8. Конвенція про кіберзлочинність від 23 листопада 2001 р. *Офіційний вісник України*. 2006. № 41. Ст. 2724.
9. Mason S., Mason L. *Electronic Evidence*. 4th ed. London, LexisNexis, 2017. 934 p.
10. Mason S. *Digital Evidence and Electronic Signature Law Review*. 2004. Vol. 1, Issue 1. P. 1–13. URL: <https://journals.sas.ac.uk/deeslr/article/view/1749> (дата звернення: 09.07.2025).
11. Лук'янчиков Є. Д. Електронні докази у кримінальному провадженні: проблеми та перспективи. *Вісник кримінального судочинства*. 2020. № 1. С. 45–2.
12. Проскурін О. М. Принцип допустимості доказів у кримінальному процесі України. *Науковий вісник Національної академії внутрішніх справ*. 2019. № 2. С. 112–119.
13. Когут О. Ю. Особливості використання цифрових технологій у доказуванні. *Юридичний вісник*. 2021. № 3. С. 87–94.
14. Кримінальний процесуальний кодекс України від 13 квітня 2012 року № 4651-VI. Відомості Верховної Ради України. 2013. № 9-10, № 11–12, № 13. Ст. 88.
15. Європейський суд з прав людини. Справа «Хан проти Сполученого Королівства» (Khan v. The United Kingdom). Рішення від 12 травня 2000 року. Заява № 35394/97.
16. Європейський суд з прав людини. Справа «Барбулеску проти Румунії» (Barbulescu v. Romania). Рішення від 05 вересня 2017 року. Заява № 61496/08.
17. Харитонов Є. О. Дотримання принципу «належної правової процедури» при використанні електронних доказів: європейські стандарти та українські реалії. *Актуальні проблеми держави і права*. 2018. Вип. 81. С. 98–105.
18. Конвенція про захист прав людини і основоположних свобод від 04 листопада 1950 року. *Офіційний вісник України*. 2006. № 32. Ст. 2371.

**Horielova V. Yu., Gorelkina K. G. AUTHENTICITY AS A CRITERION FOR THE ADMISSIBILITY OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS: COMPARATIVE ANALYSIS AND DIRECTIONS FOR IMPROVEMENT**

*The article provides a thorough study of the complex and multifaceted phenomenon of the use of digital evidence in criminal procedure in Ukraine. This topic is gaining critical importance and strategic significance in the context of the growing digitalisation of society and the evolving threats of cybercrime. The main focus is on identifying the key legal, regulatory and procedural challenges that arise when integrating electronic evidence into the national judicial system.*

*The article provides a methodological analysis of the prerequisites and criteria for ensuring the authenticity and admissibility of digital evidence sources, which are the determining factors of their legal significance and ability to influence the effectiveness of criminal proceedings. Gaps, inconsistencies, and legal conflicts in the current legislation that impede the proper regulatory consolidation of procedures for the collection, processing, preservation, and procedural use of digital evidence have been examined.*

*Particular attention is paid to an in-depth comparative analysis of international legal acts, in particular the provisions of the Council of Europe Convention on Cybercrime, and the practice of introducing electronic evidence in foreign jurisdictions. An analysis of the experience of the European Union, the United Kingdom, Canada, and Estonia has made it possible to identify effective models for creating specialised units and developing technical protocols for recording and verifying digital traces.*

*Based on the findings of the study, a set of systemic recommendations has been formulated to improve the Ukrainian criminal procedural legislation. They include a clear legislative definition of the concept of digital evidence, the creation of a regulatory classification of its forms, the introduction of unified authentication and admissibility procedures, and the institutionalisation of specialised expertise of digital sources. The results of the study make a significant contribution to the formation of a conceptually updated model of digital justice in Ukraine.*

**Key words:** digital evidence, electronic evidence, criminal procedure, authenticity of evidence, admissibility of evidence, cybercrime, forensic examination, cybersecurity.

Дата надходження статті: 10.09.2025

Дата прийняття статті: 01.10.2025

Опубліковано: 15.12.2025