**DOI https://doi.org/10.30525/978-9934-26-686-7-2**

# АВТЕНТИЧНІСТЬ І ДОПУСТИМІСТЬ ЦИФРОВИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ КРІЗЬ ПРИЗМУ ПРИНЦИПІВ КРИМІНАЛЬНОГО ПРОЦЕСУ

**Волошина В. К.**

## ВСТУП

Стрімкий розвиток цифрових технологій наприкінці XX – на початку XXI століття суттєво трансформував характер суспільних відносин, способи комунікації та форми соціальної взаємодії. Ці процеси безпосередньо вплинули і на сферу кримінального судочинства, оскільки значна частина суспільно небезпечних діянь почала вчинятися із використанням інформаційно-комунікаційних технологій або залишати після себе цифрові сліди. У таких умовах традиційні уявлення про докази, джерела доказової інформації та механізми їх процесуальної оцінки зазнали істотного переосмислення.

Цифрові докази поступово перетворилися на один із ключових елементів доказування у кримінальному провадженні. Дані електронних пристроїв, серверів, телекомунікаційних мереж, хмарних сховищ, соціальних платформ та інформаційних систем дедалі частіше використовуються для встановлення фактичних обставин кримінальних правопорушень. Водночас особлива природа такої інформації зумовлює підвищену вразливість цифрових доказів до втручання, модифікації, копіювання та знищення, що ускладнює процес підтвердження їх достовірності та процесуальної надійності.

На відміну від матеріальних чи письмових доказів, цифрові дані не мають стабільної фізичної форми, а їх сприйняття можливе виключно за допомогою спеціальних технічних засобів і програмного забезпечення. Ця обставина зумовлює необхідність застосування особливих процесуальних та технічних механізмів для забезпечення незмінності інформації з моменту її виявлення до безпосереднього дослідження судом. У протилежному випадку виникають обґрунтовані сумніви щодо автентичності цифрових доказів, що прямо впливає на можливість їх використання у процесі доказування.

Особливої актуальності проблема автентичності та допустимості цифрових доказів набуває у контексті дотримання фундаментальних принципів кримінального процесу. Принцип законності вимагає, щоб отримання електронної інформації здійснювалося виключно в межах та у спосіб, передбачений законом. Презумпція невинуватості покладає на сторону обвинувачення обов'язок довести не лише факт існування цифрового доказу, але й його достовірність, цілісність та зв'язок із конкретною подією кримінального правопорушення. Принцип змагальності сторін передбачає реальну можливість перевірки та оскарження цифрових доказів стороною захисту, у тому числі шляхом проведення альтернативних експертиз.

Окремої уваги потребує співвідношення використання цифрових доказів із правом особи на повагу до приватного життя та таємниці комунікацій.

Отримання доступу до електронних пристроїв, особистих акаунтів або хмарних сервісів нерідко пов'язане з глибоким втручанням у приватну сферу особи, що вимагає ефективного судового контролю та чіткого процесуального регулювання. Недотримання цих вимог може призвести до порушення стандартів справедливого судового розгляду, навіть за наявності технічно достовірної доказової інформації.

У зв'язку з цим проблема забезпечення автентичності та допустимості цифрових доказів виходить за межі суто технічних питань і набуває комплексного правового характеру. Вона охоплює доктринальні підходи до розуміння природи цифрових доказів, процесуальні гарантії їх отримання та оцінки, а також практику національних і міжнародних судових інституцій. Саме в цій площині формується необхідність вироблення цілісного підходу до цифрових доказів як елементу сучасного кримінального процесу.

Метою даного дослідження є комплексний аналіз автентичності та допустимості цифрових доказів у кримінальному процесі крізь призму принципів кримінального судочинства, а також визначення основних напрямів удосконалення процесуальних механізмів роботи з електронною доказовою інформацією з урахуванням сучасних викликів цифрового середовища.

## 1. Передумови виникнення проблеми автентичності та допустимості цифрових доказів

Формування проблематики автентичності та допустимості цифрових доказів у кримінальному процесі є прямим наслідком глибинних змін у способах фіксації, зберігання та передачі інформації в сучасному суспільстві. Якщо в «класичному» кримінальному судочинстві доказова діяльність ґрунтувалася переважно на матеріальних об'єктах і безпосередньо сприйманих джерелах інформації, то в умовах цифровізації дедалі більша частина релевантних відомостей існує у нематеріальній формі й опосередковується технічними системами[1].

Поява цифрових слідів як результату функціонування інформаційних систем істотно розширила доказовий простір кримінального провадження. Електронні журнали подій, мережеві логи, метадані файлів, дані геолокації, цифрові записи комунікацій та інша електронна інформація дедалі частіше стають важливими джерелами даних про підготовку, вчинення та приховування кримінальних правопорушень[2]. Водночас використання таких даних у процесі доказування супроводжується низкою специфічних проблем від складності технічної фіксації до невизначеності процесуальних стандартів їх оцінки.

Однією з базових передумов виникнення досліджуваної проблеми є відсутність матеріальної стабільності цифрових доказів. На відміну від речових доказів, цифрова інформація не має сталої фізичної форми, її існування

[1] Петрик В.В. Використання електронних доказів у кримінальному провадженні // *Науковий вісник Ужгородського Національного Університету*. Серія «Право». Випуск 87: частина 4. (2025)// URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/03/19-3.pdf

[2] ResearchGate. (2025). Electronic evidence in criminal proceedings of Ukraine. URL: https://www.researchgate.net/publication/392347214_Electronic_evidence_in_criminal_proceedings_of_Ukraine

залежить від технічного середовища та умов зберігання. Будь-яке втручання в інформаційну систему як навмисне, так і випадкове може призвести до зміни змісту даних без очевидних зовнішніх слідів, що ускладнює відтворення їх первісного стану та породжує сумніви щодо автентичності. Саме тому в літературі наголошується на необхідності розроблення чітких процедур збирання, збереження й верифікації цифрових доказів [3].

Ще однією суттєвою передумовою проблеми є опосередкований характер сприйняття цифрових доказів судом. Суд, як правило, не має можливості «безпосередньо» дослідити цифрову інформацію без залучення технічних засобів або спеціалістів, а отже значною мірою покладається на результати експертиз, висновки фахівців і внутрішні процедури провайдерів послуг. За відсутності чітко визначених процесуальних стандартів така довіра ризикує бути суто декларативною й не гарантує належного рівня процесуальної справедливості, зокрема права сторони захисту на ефективну перевірку доказів.

Важливим чинником загострення проблеми є транснаціональний характер цифрового середовища. Дані, що мають доказове значення, часто зберігаються на серверах за межами національної юрисдикції або перебувають під контролем приватних транснаціональних компаній. Це ускладнює дотримання національних процесуальних вимог щодо їх отримання, створює ризики порушення принципу законності та ставить під сумнів допустимість таких доказів у межах внутрішнього кримінального процесу. Додаткові питання виникають у зв'язку з необхідністю узгодження вимог кримінального процесуального законодавства з режимом захисту персональних даних та стандартами права на приватне життя.

Окремо слід відзначити, що чинне кримінальне процесуальне законодавство України, як і законодавство багатьох інших держав, здебільшого не містить комплексного регулювання, спрямованого саме на роботу з цифровими доказами. Наявні норми мають загальний характер і нерідко застосовуються за аналогією до матеріальних або письмових доказів, що не враховує специфіку електронної інформації, її крихкість та залежність від технічного середовища. Унаслідок цього правозастосовна практика набуває фрагментарного характеру, а критерії допустимості цифрових доказів тлумачаться судами по-різному.

У науковій доктрині також немає єдності щодо самого поняття «цифровий (електронний) доказ». Частина авторів пропонує розглядати його як різновид електронного документа, інші як окрему, самостійну категорію доказових

[3] Романюк В.В., Абламський С.Є. Критерії допустимості цифрових (електронних) доказів у кримінальному провадженні // *Law and Safety*. 2024. № 2 (93) // URL: https://pb.univd.edu.ua/index.php/PB/article/download/818/653; Шульга В., Калюжна, Л. Електронні докази у кримінальному процесі: методи їх виявлення, дослідження та правове закріплення //*Теорія та практика судової експертизи і криміналістики*. Вип. 3 (40). С. 136–152. DOI: 10.32353/khrife.3.2025.10. ; Shyshenko A. A. Digital evidences in criminal proceedings: problems of authenticity and admissibility // *Journal of Law and Social Policy*. 2025.

засобів, що потребує автономного процесуального режиму[4]. Така доктринальна розбіжність ускладнює вироблення уніфікованих підходів до встановлення автентичності цифрових доказів і створює передумови для суперечливої судової практики, зокрема щодо визначення належного джерела, способу отримання й допустимого рівня технічного втручання.

У сукупності зазначені обставини свідчать, що проблема автентичності та допустимості цифрових доказів має системний характер і не може бути вирішена виключно за рахунок удосконалення технічних методів роботи з електронними даними. Вона потребує комплексного правового осмислення з урахуванням засад кримінального процесу, які визначають межі допустимого втручання держави у сферу приватних прав і свобод особи, а також стандартів справедливого судового розгляду, сформованих, зокрема, у практиці ЄСПЛ.

Саме в цій площині постає наукова проблема, що полягає у відсутності цілісного процесуального підходу до забезпечення автентичності цифрових доказів як передумови їх допустимості у кримінальному судочинстві. Невирішеність цієї проблеми створює ризики як для ефективності кримінального переслідування (через втрату або дискредитацію важливої цифрової інформації), так і для дотримання стандартів справедливого судового розгляду, включно з правом на захист і правом на повагу до приватного життя [5].

Вважаємо, що ускладнення роботи з цифровими доказами зумовлене не лише їх технічною специфікою, але й невідповідністю класичних процесуальних конструкцій новим формам доказової інформації. Традиційні підходи до доказування формувалися в умовах, коли джерело доказу та носій інформації були тісно пов'язані між собою. У цифровому середовищі такий зв'язок втрачає стабільність, оскільки одна й та сама інформація може одночасно існувати на кількох носіях, змінювати форму відображення та передаватися без фізичного контакту з оригінальним пристроєм.

Ця особливість зумовлює виникнення принципово нового для кримінального процесу питання, що саме слід вважати "оригіналом" цифрового доказу. На відміну від матеріальних об'єктів, де автентичність пов'язується з фізичною унікальністю предмета, у цифровому середовищі копія може бути технічно ідентичною первинному файлу. Як зазначає S. Mason, «it is important to obtain

[4] Квашук О.Д. Використання електронних доказів у кримінальному провадженні // *Центральноукраїнський вісник права та публічного управління.* Випуск/ Issue 2(10),2025.С. 50–56.; Романюк В.В., Абламський С.Є. Критерії допустимості цифрових (електронних) доказів у кримінальному провадженні // *Law and Safety*. 2024. № 2 (93) // URL: https://pb.univd.edu.ua/index.php/PB/article/download/818/653 ; Шульга В., Калюжна, Л. Електронні докази у кримінальному процесі: методи їх виявлення, дослідження та правове закріплення// *Теорія та практика судової експертизи і криміналістики.* Вип. 3 (40). С. 136–152. DOI: 10.32353/khrife.3.2025.10.; Метелев О.П., Цифрові докази у кримінальному процесі: видова характеристика // *Вісник кримінального судочинства* № 1–2, 2023. С.42-53. DOI: https://doi.org/10.17721/2413-5372.2023.1-2/42-53

[5] The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations. 2022. SSRN.

the item in the native format… as this is the only way… integrity… can be proven»[6]. За відсутності чітких процесуальних критеріїв це створює підґрунтя для сумнівів щодо достовірності доказів та відкриває можливості для зловживань у процесі їх подання і дослідження.

Ще одним важливим аспектом є розрив між технічною та юридичною автентичністю цифрових доказів. Навіть за умови, що з технічної точки зору дані не зазнали змін (що підтверджується, наприклад, хеш-значенням), це саме по собі не гарантує їх допустимості у кримінальному процесі. Юридична автентичність передбачає встановлення походження інформації, законність способу її отримання, а також дотримання процесуальних гарантій прав учасників провадження. Як зазначає І. Липкан, «інформація… має специфічну технічну природу, що забезпечує її автентичність і можливість дослідження».[7] Таким чином, технічна цілісність даних є лише однією з умов їх допустимості, але не може розглядатися як самодостатній критерій.

У цьому контексті особливої ваги набуває принцип законності, який виступає фундаментальною засадою кримінального процесу. Отримання цифрових доказів поза межами процесуальної форми, навіть за наявності їх фактичної достовірності, ставить під сумнів можливість їх використання у судовому розгляді. Практика свідчить, що порушення процедури доступу до електронних пристроїв або інформаційних систем часто призводить до визнання відповідних доказів недопустимими, оскільки такі порушення мають істотний характер і впливають на баланс між публічним інтересом та правами особи. Міжнародні стандарти підтверджують цю позицію: держави повинні забезпечувати процедури отримання електронних даних із дотриманням гарантій прав людини, включаючи «judicial or other independent supervision… limitation of the scope and the duration».[8]

Не менш значущою передумовою формування проблеми є обмежена здатність сторони захисту впливати на процес перевірки цифрових доказів. Європейський суд з прав людини наголошує, що «electronic evidence has become ubiquitous in criminal trials», а тому його оцінка повинна здійснюватися з урахуванням принципу справедливого судового розгляду.[9] У багатьох випадках цифрові дані вилучаються, копіюються та аналізуються без активної участі захисту, що ускладнює реалізацію принципу змагальності сторін. За відсутності належних процесуальних механізмів контролю за діями сторони

[6] Mason S. Electronic Evidence and Electronic Signatures. 5th ed. London: Institute of Advanced Legal Studies, 2021. URL: https://sas-space.sas.ac.uk/9564/1/9781911507246_min.pdf

[7] Липкан І.І. Особливості доказування у справах про шахрайство, вчинене з використанням цифрових технологій: дис. … д-ра юрид. наук. Київ, 2025. URL: https://dpu.edu.ua/images/Documents/NAUKA/Doktorski%20specializovani%20vceni%20radi/Specializovana%20vcena%20rada%20D%2027.855.03/Lipkan%20Igor%20Ivanovic/Disertacia%20Lipkana%20I.I.pdf

[8] Convention on Cybercrime (Budapest Convention). Council of Europe, 2001. URL: https://rm.coe.int/1680081561

[9] European Court of Human Rights. Background Paper for the Judicial Seminar 2025. Strasbourg, 2024. URL: https://www.echr.coe.int/documents/d/echr/seminar-background-paper-2025-eng

обвинувачення виникає ризик одностороннього формування доказової бази, що суперечить засадам справедливого судового розгляду.

Особливу складність становить і питання оцінки цифрових доказів судом. Як зазначають А. Політова та Т. Чехлай, «КПК України не містить згадки щодо електронних доказів», що створює прогалини у правовому регулюванні[10]. Судова практика демонструє відсутність єдиних підходів до визначення критеріїв допустимості електронної інформації. В одних випадках пріоритет надається технічним характеристикам доказу, в інших процесуальним аспектам його отримання. Така непослідовність створює правову невизначеність і підриває передбачуваність судових рішень, що є несумісним із принципом правової визначеності.

З огляду на викладене, проблема автентичності та допустимості цифрових доказів не може бути зведена до окремих недоліків правового регулювання чи прогалин у технічному забезпеченні слідчої діяльності. Вона має комплексний характер, охоплюючи доктринальний, нормативний і правозастосовний рівні кримінального процесу. Відсутність узгодженого підходу до розуміння цифрових доказів і стандартів їх оцінки негативно впливає як на ефективність розслідування кримінальних правопорушень, так і на рівень гарантій прав людини.

У зв'язку з цим наукова проблема дослідження полягає у необхідності вироблення цілісної процесуальної концепції забезпечення автентичності цифрових доказів, яка б ґрунтувалася на принципах кримінального судочинства та враховувала особливості цифрового середовища. Формулювання такої концепції є передумовою створення єдиних критеріїв допустимості електронної доказової інформації та підвищення якості судової оцінки цифрових доказів.

Таким чином, виникнення передумов проблеми та її формулювання свідчать про необхідність переходу від фрагментарного використання технічних інструментів до системного правового підходу, який поєднує технічні, процесуальні та правозахисні елементи. Саме цей підхід дозволяє розглядати цифрові докази не як виняток із загальних правил доказування, а як повноцінний інститут сучасного кримінального процесу.

## 2. Правова природа та поняття цифрових доказів у кримінальному процесі.

Правова природа та поняття цифрових (електронних) доказів у кримінальному процесі України є одним з найбільш актуальних і динамічних напрямів сучасного кримінально-процесуального права. Розвиток інформаційних технологій, масове використання цифрових пристроїв, мереж Інтернет, мобільних застосунків, хмарних сервісів та соціальних платформ призвели до появи принципово нових джерел доказової інформації, які не завжди вписуються в традиційну систему процесуальних джерел доказів, передбачену ч. 2 ст. 84 Кримінального процесуального кодексу України (далі КПК України). Процес доказування супроводжує всю стадію досудового розслідування від внесення

[10] Політова А.С., Чехлай Т.О. Допустимість цифрових доказів у кримінальному провадженні: аналіз судової практики. *Вісник МДУ. Серія: Право*. 2025. № 29. С. 104–115.

відомостей до Єдиного реєстру досудових розслідувань до прийняття остаточного рішення у кримінальному провадженні. Перевірка, оцінка та належне закріплення доказів здійснюється особою, яка проводить розслідування, з метою забезпечення того, щоб зібрані матеріали лягли в основу законного та обґрунтованого рішення. Якщо традиційні докази (показання, речові докази, документи, висновки експертів) переважно мають матеріальну або паперову форму, то електронні (цифрові) докази існують у нематеріальній, цифровій формі, що створює суттєві труднощі щодо їх фіксації, збереження цілісності, перевірки автентичності та оцінки допустимості. Питання правової природи, поняття та використання електронних (цифрових) доказів активно вивчаються українськими науковцями. Серед ключових праць дослідження О. Сіренко, В. Хахановського та М. Гуцалюка, А. Столітнього та І. Каланчі, О. Козицької, О. Метелєва, Д. Алексєєвої-Працюк, М. Гуцалюка та П. Антонюка, А. Коваленка, Л. Перцової-Тодорової, Г. Татаренка та ін., А. Антонюка та В. Русецької, В. Школьнікова.

Після 2021 р. дискусія набула нового імпульсу завдяки прийняттю Закону України від 15.03.2022 № 2137-IX «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам», який суттєво розширив можливості роботи з електронними доказами в умовах кіберзлочинності та воєнного стану. Сучасні дослідження підкреслюють необхідність визнання електронних доказів самостійною групою джерел доказів, матеріали круглих столів та монографій з цифровізації кримінального провадження.

Інформаційні технології зумовили постійну необхідність передачі та обміну даними. Використання електронних пристроїв стало щоденною практикою, але паралельно зросла кількість правопорушень у цифровій сфері. Оскільки дані існують в електронній формі, механізм їх фіксації як доказів має процедурні особливості.

У доктрині сформувалося кілька підходів до розуміння правової природи та поняття цифрових (електронних) доказів.

**Перший (розширений, функціональний) підхід** розглядає електронні докази як будь-яку інформацію в цифровій формі, що має значення для встановлення обставин провадження, незалежно від конкретного джерела. О. Козицька визначала їх як цифрові об’єкти, що були засобом чи знаряддям вчинення злочину, зберегли електронно-цифрові сліди, були предметом чи об’єктом правопорушення або містять відомості, які можуть бути використані як доказ[11]. Аналогічно О. Сіренко наголошувала на необхідності законодавчого закріплення поняття «електронні докази» в КПК[12] .

**Другий (техніко-ознаковий) підхід** акцентує специфічні властивості: нематеріальний вигляд; неможливість існування поза технічним носієм або каналом зв’язку; вільне переміщення в мережі; сприйняття лише за допомогою

[11] Козицька О.Г. Щодо поняття електронних доказів у кримінальному провадженні // *Юридичний науковий електронний журнал*. 2020. № 8. С. 418–421.

[12] Сіренко О.В. Електронні докази у кримінальному провадженні // *Міжнародний юридичний вісник*. 2019. № 14. С. 208–214.

техніки та ПЗ; потреба в спеціальному порядку збирання, перевірки, оцінки; можливість дистанційного внесення змін чи видалення[13].

**Третій (інтеграційний, сучасний) підхід** пропонує визнати електронні докази окремою самостійною групою, відмінною від показань, речових доказів, документів та висновків експертів[14]. О. Метелєв наголошував на необхідності виділення спеціальних слідчих дій «цифровий огляд інформаційного середовища» та «цифрове копіювання»[15]. Пропонується закріпити окрему статтю КПК (наприклад, ст. 99-1) з визначенням цифрових доказів як відомостей або документів у цифровій/електронній формі, отриманих під час досудового розслідування чи ОРД.

У сучасній доктрині переважає погляд, що електронні (цифрові) докази – це інформація в електронній (цифровій) формі про факти та обставини кримінального провадження, зафіксована в електронних документах, текстових, мультимедійних, голосових повідомленнях, метаданих, базах даних тощо, яка зберігається на електронних носіях (мобільні пристрої, сервери, карти пам'яті, USB-накопичувачі, хмарні сховища), вільно переміщується в мережі, не має нерозривного зв'язку з матеріальним носієм, потребує спеціального порядку збирання, перевірки та оцінки, сприймається лише за допомогою технічних засобів і ПЗ.

Авторське визначення, запропоноване в сучасних дослідженнях[16]: електронний доказ у кримінальному процесі це інформація про факти та обставини кримінального провадження, зафіксована в електронній (цифровій) формі, отримана в передбаченому КПК порядку, відмінна від доказів в електронному вигляді та така, що характеризується нематеріальною природою, залежністю від технічних засобів та специфічними ризиками зміни/втрати цілісності.

Джерела електронних доказів багатоманітні та не вичерпні: електронні документи (за Законом «Про електронні документи та електронний документообіг»; сайти, електронні бази даних, файли, електронна пошта, чати, сервери; записи з камер відеоспостереження, реєстраторів, застосунків на мобільних пристроях; дані з відкритих джерел (OSINT); матеріали з міжнародної правової допомоги тощо.

---

[13] Алексєєва-Працюк Д. та ін. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування // *Науковий вісник публічного та приватного права*. 2018. № 2. С. 252.; Гуцалюк М.В., Антонюк П.Є. Щодо сутності електронної (цифрової) інформації як джерел доказів у кримінальному провадженні // *Криміналістичний вісник*. 2020. № 1. С. 42.

[14] Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України // *Проблеми законності*. 2019. № 146. С. 179.; Антонюк А.Б., Русецька В.А. Електронні докази в кримінальному провадженні // *Міжнародний науковий журнал «Інтернаука».* 2020. № 10. С. 85.

[15] Метелев О.П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження // *Науковий вісник Ужгородського національного університету*. 2020. № 60. С. 177.

[16] Мілімко Л.В. Електронні докази в кримінальному судочинстві України // *Науковий вісник УжНУ*. Серія «Право». 2025. (або рік видання за фактом публікації).

Принципи, що характеризують електронні докази: допустимість, справжність (автентичність), повнота, надійність, зрозумілість, правдоподібність[17].

Правова природа цифрових доказів є комплексною: вони поєднують ознаки документа (якщо оформлені належним чином), речового доказу (якщо вилучено носій) та специфічної інформаційної категорії, що потребує самостійного регулювання. Відсутність легального визначення в КПК України (на відміну від ЦПК, ГПК, КАС) залишається ключовою проблемою, яка ускладнює єдність практики, особливо в умовах воєнного стану та зростання кіберзлочинності.

**Отже,** електронні (цифрові) докази є невід'ємною частиною сучасного кримінального провадження, їх роль зростає в розслідуванні кіберзлочинів, воєнних злочинів, злочинів проти національної безпеки. Вони характеризуються нематеріальною формою, залежністю від технічних засобів, ризиками маніпуляцій, потребують спеціальних процедур збирання, фіксації (з дотриманням chain of custody), перевірки та оцінки.

Вважаємо, що доцільно доповнити КПК України окремою статтею про електронні (цифрові) докази, визначити їх поняття, ознаки, порядок збирання, перевірки, оцінки та використання, передбачити спеціальні слідчі дії щодо роботи з цифровою інформацією, врахувати міжнародні стандарти. Це дозволить усунути невідповідності, підвищити ефективність розслідування та забезпечити права учасників провадження.

## 3. Процесуальні принципи забезпечення допустимості цифрових доказів

Подальший розвиток процесуально-правового підходу до оцінки цифрових доказів неможливий без поглибленого аналізу принципу законності як базового критерію їх допустимості. У сфері цифрових доказів цей принцип набуває специфічного змісту, оскільки будь-яке втручання у функціонування електронних пристроїв, інформаційних систем або мереж пов'язане з потенційним обмеженням конституційних прав особи. Законність у такому контексті передбачає не лише наявність формальної правової підстави для проведення слідчої (розшукової) дії, а й реальне дотримання визначеної законом процедури доступу до цифрових даних, включно із судовим контролем, фіксацією кожного етапу роботи з інформацією та дотриманням принципу пропорційності[18].

Порушення процесуальної форми під час отримання електронної інформації нерідко має латентний характер і не завжди очевидне на стадії судового розгляду. Тому вимога законності виступає не лише критерієм оцінки діяльності органів досудового розслідування, а й ключовою гарантією захисту

[17] Метелев О.П. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процесі // *Вісник кримінального судочинства*. 2019. № 3. С. 234–235.

[18] Квашук О.Д. Використання електронних доказів у кримінальному провадженні // *Центральноукраїнський вісник права та публічного управління.* Випуск/ Issue 2(10), 2025. С. 50–56.

від свавільного втручання в приватну сферу. Якщо цифрові докази здобуті без належного судового контролю чи з перевищенням повноважень, їх використання в кримінальному провадженні суперечить змісту принципу законності незалежно від їх доказової ваги.

Тісно пов'язаний із законністю принцип презумпції невинуватості визначає загальну логіку розподілу тягаря доказування. У контексті цифрових доказів він означає, що будь-які обґрунтовані сумніви щодо автентичності, походження чи цілісності електронної інформації мають тлумачитися на користь особи, щодо якої здійснюється кримінальне переслідування. Відповідно, саме сторона обвинувачення повинна довести, що відповідні цифрові дані не зазнали несанкціонованих змін, не були сфальсифіковані й отримані з дотриманням процесуальних вимог, а ланцюг їх збереження є безперервним.

Особливість цифрових доказів полягає в тому, що їх технічна складність і залежність від спеціальних знань створюють відчутну асиметрію між сторонами кримінального провадження. Органи досудового розслідування зазвичай мають доступ до значно ширших технічних ресурсів і експертного потенціалу, ніж сторона захисту. У таких умовах презумпція невинуватості фактично виконує компенсаторну функцію, покликану запобігти перекладанню на захист обов'язку доводити недостовірність чи фальсифікацію цифрових доказів до того, як їх автентичність буде належним чином обґрунтована стороною обвинувачення.

Не менш важливим у цьому контексті є принцип змагальності сторін, який передбачає реальну, а не формальну можливість кожної зі сторін брати участь у дослідженні доказів. Стосовно цифрових доказів це означає забезпечення доступу захисту до копій відповідних електронних носіїв, інформації про використані методи й програмні засоби, а також створення умов для ініціювання альтернативних чи повторних експертиз. За відсутності таких можливостей змагальність перетворюється на декларацію, а висновки експертів набувають характеру фактично неоспорюваних, що підриває довіру до результатів судового розгляду.

На практиці обмеження доступу захисту до цифрових доказів часто мотивується міркуваннями безпеки або ризиком втручання у дані. Водночас подібні аргументи не можуть мати універсального характеру і автоматично виправдовувати істотне звуження процесуальних прав захисту. Баланс між необхідністю збереження цілісності цифрових даних і забезпеченням реальної змагальності має досягатися через запровадження чітких процесуальних гарантій (створення форензичних копій, використання сертифікованих інструментів, фіксацію кожної операції), а не шляхом односторонніх заборон.

Окремого розгляду потребує право на захист як комплексна процесуальна гарантія, що охоплює можливість своєчасного ознайомлення з доказами, участі в слідчих діях, використання спеціальних знань та залучення фахівців для критичної оцінки цифрової інформації. У сфері цифрових доказів реалізація цього права ускладнюється як технічними бар'єрами, так і відсутністю деталізованих процедур, які б регламентували доступ захисника до електронних даних та його участь у їх дослідженні. У підсумку існує ризик, що

суттєві цифрові докази фактично залишаться поза дієвим судовим контролем, навіть за формального дотримання процесуальної форми.

Узагальнюючи викладене, слід констатувати, що наявні підходи до вирішення проблеми автентичності та допустимості цифрових доказів є фрагментарними і не забезпечують повної реалізації засад кримінального процесу. Технічні засоби фіксації та захисту даних, хоч і відіграють важливу роль, не можуть замінити процесуальні гарантії й самі по собі не гарантують справедливості судового розгляду. Ефективна модель оцінки цифрових доказів можлива лише за умови органічного поєднання технічних і правових елементів у межах цілісного процесуального підходу.

У цьому зв'язку завдання дослідження полягає у виробленні узгодженого підходу до допустимості цифрових доказів, який поєднував би вимоги технічної автентичності з принципами законності, презумпції невинуватості, змагальності сторін та належної реалізації права на захист. Запровадження такого підходу має сприяти підвищенню рівня правової визначеності, зменшенню ризику довільного тлумачення критеріїв допустимості й забезпеченню балансу між ефективністю кримінального переслідування та дотриманням прав людини.

Завершуючи аналіз існуючих підходів до проблеми автентичності та допустимості цифрових доказів, варто наголосити, що жоден із них у відокремленому вигляді не відповідає всім викликам сучасного кримінального процесу. Техніко-орієнтований підхід, попри очевидні переваги у сфері фіксації та збереження електронної інформації, недостатньо відображає процесуальний вимір доказування. Процесуально-правовий підхід, навпаки, спирається на фундаментальні засади судочинства, але часто лишається занадто загальним і не враховує особливостей цифрового середовища.

Саме тому особливого значення набуває питання узгодження технічних стандартів роботи з цифровими даними з процесуальними вимогами кримінального провадження. Цифрові докази мають оцінюватися не лише з погляду їх інформаційної цінності чи технічної цілісності, а й з урахуванням того, чи був дотриманий належний процесуальний порядок на всіх етапах від виявлення й вилучення до дослідження в суді. Відсутність уніфікованих критеріїв допустимості, які послідовно застосовувалися б як слідчими, так і судами, породжує правову непевність: у подібних ситуаціях ідентичні за природою цифрові дані можуть оцінюватися по-різному.

Міжнародний вимір проблеми зумовлений тим, що цифрові докази дедалі частіше мають транснаціональний характер. Доступ до даних, що зберігаються за кордоном або контролюються іноземними сервіс-провайдерами, ставить перед правозастосовними органами складні завдання, пов'язані з дотриманням принципу законності та міжнародних стандартів захисту прав людини. За таких умов оцінка допустимості цифрових доказів повинна здійснюватися з урахуванням не лише внутрішнього процесуального законодавства, а й відповідних міжнародних зобов'язань держави.

Важлива роль у цій системі належить суду як остаточному арбітру у питаннях допустимості цифрових доказів. Судова перевірка не може обмежуватися виключно формальним контролем наявності ухвал, протоколів

чи технічних звітів. Її змістом має стати з'ясування того, чи забезпечено у конкретній справі реальне дотримання засад справедливого судового розгляду, рівності сторін та права на ефективний захист. Такий підхід дозволяє уникнути надмірного формалізму і підтримати баланс між інтересами правосуддя та правами особи.

З огляду на це завдання даного дослідження полягає у формуванні інтегрованого процесуального підходу до автентичності та допустимості цифрових доказів, який поєднає технічні механізми забезпечення цілісності електронних даних із вимогами основних принципів кримінального процесу. Такий підхід має ґрунтуватися на чітких критеріях законності отримання цифрової інформації, обґрунтованому розподілі тягаря доказування автентичності між сторонами, а також на реальному забезпеченні змагальності й права на захист при дослідженні цифрових доказів у суді. Його впровадження створює підґрунтя для підвищення ефективності кримінального судочинства в умовах цифровізації та одночасно гарантує належний рівень захисту прав людини, дозволяючи розглядати цифрові докази як повноцінний інститут сучасного кримінального процесу.

## 4. Міжнародні стандарти допустимості цифрових доказів та практика ЄСПЛ

Стрімкий розвиток цифрових технологій спричинив не лише трансформацію національних підходів до доказування у кримінальному процесі, а й формування міжнародних стандартів роботи з електронними доказами. З огляду на транснаціональний характер кіберпростору та глобальну природу цифрових даних, питання їх отримання, фіксації та оцінки дедалі частіше виходять за межі національної юрисдикції[19]. У таких умовах узгодження внутрішніх процесуальних механізмів із міжнародними правовими стандартами набуває критичного значення.

Одним із фундаментальних міжнародних актів у сфері боротьби з кіберзлочинністю та роботи з цифровими доказами є Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція, 2001 р.)[20]. Цей документ став першим універсальним інструментом, що визначив правові засади міжнародного співробітництва у виявленні, збереженні та отриманні електронних доказів. Статті 16–22 Конвенції детально регламентують принципи оперативного збереження комп'ютерних даних, процедури доступу до інформації в комп'ютерних системах, а також механізми транскордонної взаємодії при розслідуванні злочинів у цифровому середовищі[21].

Особливістю Будапештської конвенції є системний підхід до цифрових доказів як об'єкта, що вимагає одночасного дотримання як технічних, так і правозахисних стандартів (ст. 15)[22]. Конвенція прямо передбачає необхідність

[19] Гутник Х. М., Хитра О. В. Цифрові докази у кримінальному процесі : монографія. Львів: ЛДУВС України, 2022. 248 с.

[20] Конвенція Ради Європи про кіберзлочинність від 23.11.2001 № 185 (ETS № 185). Ратифікована Законом України № 608-III від 21.09.2005.

[21] Там само, ст. 16–22.

[22] Там само, ст. 15.

пропорційності втручання у приватне життя, що унеможливлює використання електронної інформації, отриманої з порушенням базових процесуальних гарантій.

Подальший розвиток міжнародних стандартів пов'язаний із правом Європейського Союзу, зокрема Регламентом (ЄС) 2023/1543 про Європейську виробничу ордерну систему (e-Evidence Regulation)[23]. Цей документ запровадив концепцію європейських ордерів на отримання електронних доказів, що передбачає спрощені процедури транскордонного доступу до даних, зберігаючи при цьому високі стандарти захисту прав людини. Допустимість електронної інформації тут оцінюється комплексно через призму як технічної цілісності (хеш-сум, ланцюг збереження), так і законності отримання з належним судовим контролем[24].

Важливе місце посідають і міжнародні стандарти поводження з цифровими доказами, розроблені INTERPOL та ENFSI. Зокрема, ISO/IEC 27037:2012 (Guidelines for identification, collection, acquisition and preservation of digital evidence) наголошує на безумовній незмінності інформації та детальному документуванні кожного етапу роботи з нею[25]. Ці стандарти, попри технічний характер, тісно переплітаються з процесуальними гарантіями, забезпечуючи суду обґрунтовану довіру до цифрових доказів.

Практика Європейського суду з прав людини формує ключові критерії допустимості цифрових доказів через призму статей 6 (право на справедливий суд) та 8 Конвенції (повага до приватного життя)[26]. Хоча ЄСПЛ не розробив спеціальної доктрини «цифрових доказів», його позиція чітка: допустимість є прерогативою національного права, але загальна справедливість провадження залишається під контролем Конвенції[27].

У рішенні *Demirhan v. Turkey* (2025)[28] Суд визнав порушення ст. 6 §1 через використання мобільних метаданних без належного судового контролю, попри їх технічну достовірність. ЄСПЛ підкреслив, що масове отримання електронних даних без конкретизації обґрунтування є непропорційним втручанням у приватне життя.

У справі *Benedittini and Others v. Italy* (2023)[29] Суд встановив порушення принципу рівності сторін: обвинувачення надало експертний звіт про аналіз

[23] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 27 June 2023 on European Production and Preservation Orders for electronic evidence in criminal matters // *Official Journal of the European Union.* 2023. L 168.

[24] Guidelines on the Treatment of Electronic Evidence in Criminal Proceedings. Commonwealth Secretariat. London, 2025.

[25] Information technology -Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012.

[26] Конвенція про захист прав людини і основоположних свобод від 04.11.1950 // URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

[27] *Schatschaschwili v. Germany* [GC], № 30362/08, ECHR 2015, § 101. // URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159566%22]}

[28] Demirhan v. Turkey, № 13115/21, ECHR 2025 // URL : https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-117601%22]}

[29] Benedittini and Others v. Italy, № 22152/13, ECHR 2023, § 45–52 // URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-98442%22]}

телефонних з'єднань, але відмовило захисту в доступі до сирцевих даних і програмного забезпечення. ЄСПЛ наголосив, що у цифрових доказах реальна можливість оскарження передбачає доступ до первинних носіїв та методології аналізу.

Значущою є позиція щодо доказів від приватних суб'єктів. У *Kablis v. Russia* (2021)[30] ЄСПЛ підкреслив, що отримання IP-логів від провайдера за запитом поліції не звільняє державу від обов'язку забезпечити процесуальні гарантії. Навпаки, потрібна подвійна перевірка: законність запиту до приватної компанії та пропорційність втручання.

Узагальнюючи, міжнародні стандарти та практика ЄСПЛ вимагають від національних судів комплексної оцінки цифрових доказів за такими критеріями:

1. Законність отримання (судовий контроль, пропорційність);
2. Технічна автентичність (ланцюг збереження, хеш-сум);
3. Змагальність (доступ захисту до первинних даних);
4. Загальна справедливість провадження.

Ці принципи слугують орієнтиром для гармонізації українського КПК, зокрема щодо транскордонного доступу до даних та критеріїв допустимості електронних доказів.

## 5. Особливості фіксації та забезпечення цілісності цифрових доказів у кримінальному провадженні

Ефективність використання цифрових доказів у кримінальному процесі значною мірою залежить від належної організації їх фіксації, збереження та подальшої перевірки. На відміну від традиційних доказових об'єктів, цифрова інформація характеризується високою динамічністю, можливістю миттєвого копіювання та ризиком непомітної модифікації. Саме ці властивості зумовлюють необхідність застосування спеціальних процедур, спрямованих на забезпечення незмінності електронних даних від моменту їх виявлення до дослідження судом.

Однією з ключових особливостей роботи з цифровими доказами є необхідність точної фіксації первісного стану інформації. Така фіксація передбачає не лише копіювання даних, але й документування технічних параметрів їх зберігання, структури файлової системи, метаданих та інших характеристик, що дозволяють відтворити контекст функціонування інформаційної системи. Без належної фіксації цих параметрів цифрові докази можуть втратити свою доказову цінність, оскільки стає неможливим підтвердити їх незмінність.

Важливим інструментом забезпечення цілісності цифрових доказів є створення точних цифрових копій носіїв інформації, яке здійснюється із застосуванням спеціалізованих технічних засобів. Такий процес дозволяє працювати з копією даних без ризику зміни оригінального носія. Принцип збереження оригіналу у незмінному стані є одним із базових у цифровій

[30] Kablis v. Russia, № 46118/13, ECHR 2021, § 98. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-192769%22]}

криміналістиці, оскільки будь-яке втручання в первинний носій може поставити під сумнів автентичність інформації.

Не менш важливу роль відіграє фіксація метаданих, які містять інформацію про створення, зміну та використання цифрових файлів. Метадані дозволяють встановити часові межі існування інформації, ідентифікувати користувачів, які мали доступ до даних, та відстежити історію їх змін. У багатьох випадках саме метадані виступають ключовим джерелом доказової інформації, що підтверджує або спростовує обставини кримінального правопорушення.

З метою підтвердження незмінності цифрових доказів широко застосовуються криптографічні методи контролю цілісності, зокрема використання хеш-функцій. Хеш-значення є унікальним цифровим відбитком інформації, який змінюється при будь-якому втручанні у дані. Порівняння хеш-значень, отриманих на різних етапах роботи з цифровими доказами, дозволяє встановити факт збереження або порушення їх цілісності.

Водночас технічні засоби забезпечення незмінності даних повинні доповнюватися процесуальним документуванням усіх дій, пов'язаних із цифровими доказами. Це передбачає складання протоколів вилучення, фіксацію осіб, які мали доступ до інформації, а також зазначення умов її зберігання. Така процедура формує так званий ланцюг зберігання доказів, який дозволяє простежити весь шлях цифрової інформації від моменту її виявлення до судового розгляду.

Ланцюг зберігання відіграє вирішальну роль у забезпеченні довіри до цифрових доказів. Його порушення або неповнота документування можуть створити підстави для сумнівів щодо автентичності інформації. У цьому контексті важливо забезпечити безперервність контролю за доступом до цифрових носіїв та виключити можливість несанкціонованого втручання у дані.

Особливу складність становить фіксація цифрових доказів, що зберігаються у віддалених інформаційних системах та хмарних сервісах. У таких випадках органи досудового розслідування не мають фізичного доступу до носіїв інформації, а отримання даних здійснюється через провайдерів електронних послуг. Це створює додаткові ризики втрати частини інформації або неможливості перевірки її первісного стану. У зв'язку з цим особливого значення набуває оперативність збереження даних та чітке документування процедур їх отримання.

Не менш важливим є питання забезпечення процесуальної прозорості роботи з цифровими доказами. Сторона захисту повинна мати можливість перевірити достовірність технічних процедур, що застосовувалися під час вилучення та аналізу інформації. Це передбачає доступ до копій цифрових носіїв, результатів експертних досліджень та методик, використаних при обробці даних. Забезпечення такої прозорості є необхідною умовою реалізації принципу змагальності сторін.

Важливим аспектом є також зберігання цифрових доказів протягом усього кримінального провадження. Неналежні умови зберігання можуть призвести до пошкодження носіїв інформації або втрати даних, що унеможливить їх використання у судовому розгляді. Саме тому до цифрових доказів

застосовуються підвищені вимоги щодо контролю доступу, резервного копіювання та захисту від несанкціонованого втручання.

Узагальнюючи викладене, можна зробити висновок, що забезпечення цілісності цифрових доказів є комплексним процесом, який поєднує технічні та процесуальні елементи. Лише за умови їх узгодженого застосування можливо гарантувати достовірність електронної інформації та її допустимість у кримінальному судочинстві. Відсутність належної фіксації, документування або контролю за цифровими доказами створює ризик втрати їх доказового значення та може призвести до порушення принципів справедливого судового розгляду.

Таким чином, особливості фіксації та забезпечення цілісності цифрових доказів свідчать про необхідність формування спеціалізованих процесуальних стандартів, які враховують специфіку електронної інформації та спрямовані на забезпечення балансу між ефективністю кримінального переслідування і захистом прав людини.

**ВИСНОВКИ**

Проведене дослідження дозволяє дійти висновку, що цифрові докази стали невід'ємним елементом сучасного кримінального процесу та істотно вплинули на трансформацію традиційних уявлень про доказування. Їх поява зумовлена не лише розвитком інформаційних технологій, але й зміною способів вчинення кримінальних правопорушень, значна частина яких супроводжується утворенням цифрових слідів. У таких умовах забезпечення автентичності та допустимості цифрових доказів набуває ключового значення для ефективності та справедливості кримінального судочинства.

У роботі обґрунтовано, що специфіка цифрових доказів полягає у їх нематеріальній природі, опосередкованості технічними системами та підвищеній вразливості до змін. Ці особливості зумовлюють необхідність застосування спеціальних процесуальних і технічних механізмів для підтвердження достовірності електронної інформації. Водночас встановлено, що технічна автентичність цифрових даних не може розглядатися як самодостатній критерій їх допустимості у кримінальному процесі без належного врахування процесуальних гарантій.

Аналіз передумов формування проблеми автентичності та допустимості цифрових доказів свідчить про наявність системних суперечностей між класичними процесуальними конструкціями та новими формами доказової інформації. Відсутність чітко визначеного понятійного апарату, єдиних критеріїв допустимості та уніфікованих стандартів судової оцінки цифрових доказів призводить до фрагментарності правозастосовної практики та правової невизначеності. Це, у свою чергу, негативно впливає на реалізацію принципів кримінального процесу.

У ході дослідження встановлено, що ключову роль у забезпеченні допустимості цифрових доказів відіграють принципи законності, презумпції невинуватості, змагальності сторін та забезпечення права на захист. Принцип законності визначає межі допустимого втручання держави у сферу приватних прав особи під час отримання цифрової інформації та виступає первинною

умовою використання електронних даних у процесі доказування. Порушення процесуальної форми отримання цифрових доказів, незалежно від їх фактичної достовірності, підриває легітимність таких доказів у судовому розгляді.

Презумпція невинуватості у контексті цифрових доказів виявляється у покладенні тягаря доведення їх автентичності та допустимості на сторону обвинувачення. Будь-які сумніви щодо походження, цілісності або незмінності електронної інформації мають тлумачитися на користь особи, щодо якої здійснюється кримінальне переслідування. Такий підхід сприяє підтриманню процесуальної рівноваги між сторонами та запобігає необґрунтованому використанню технічно складних доказів як засобу тиску на захист.

Принцип змагальності сторін та право на захист набувають особливої ваги у сфері цифрових доказів, оскільки їх технічна складність може створювати асиметрію процесуальних можливостей. Забезпечення реального доступу сторони захисту до цифрових носіїв, результатів експертиз і методів обробки даних є необхідною умовою ефективного судового контролю за доказами. Обмеження таких можливостей перетворює змагальність на формальність і ставить під сумнів справедливість судового розгляду.

Дослідження існуючих підходів до вирішення проблеми показало, що техніко-орієнтовані та процесуально-правові концепції мають застосовуватися не ізольовано, а у взаємозв'язку. Технічні інструменти фіксації та збереження цифрових даних повинні бути інтегровані у чітко визначену процесуальну форму, яка забезпечує дотримання прав учасників кримінального провадження. Лише за таких умов можливе формування довіри до цифрових доказів як повноцінного елементу доказової системи.

Особливу увагу в роботі приділено необхідності врахування міжнародного та транснаціонального виміру використання цифрових доказів. Зберігання електронної інформації за межами національної юрисдикції, а також участь приватних транснаціональних суб'єктів у контролі за даними вимагають адаптації національних процесуальних підходів до міжнародних стандартів захисту прав людини. У цьому контексті практика міжнародних судових інституцій слугує важливим орієнтиром для формування критеріїв допустимості цифрових доказів.

Узагальнюючи результати дослідження, можна констатувати, що забезпечення автентичності та допустимості цифрових доказів потребує формування цілісної процесуальної концепції, яка поєднує технічні, правові та правозахисні елементи. Така концепція має ґрунтуватися на принципах кримінального процесу та бути спрямованою на досягнення балансу між ефективністю кримінального переслідування і дотриманням прав людини. Реалізація зазначених підходів сприятиме підвищенню якості судового розгляду та зміцненню довіри до правосуддя в умовах цифровізації.

Проведений аналіз міжнародних стандартів допустимості цифрових доказів та практики Європейського суду з прав людини дозволяє дійти висновку, що сучасні підходи до використання електронної доказової інформації ґрунтуються на пріоритеті процесуальних гарантій прав людини. Міжнародні правові акти та судова практика формують комплексну модель оцінки цифрових доказів, відповідно до якої технічна достовірність електронних даних

не може розглядатися ізольовано від законності способу їх отримання та загальної справедливості кримінального провадження.

Встановлено, що Будапештська конвенція та інші міжнародні стандарти закріплюють принцип пропорційності втручання у приватне життя під час отримання електронної інформації, що є ключовою умовою допустимості цифрових доказів у кримінальному процесі. Практика Європейського суду з прав людини підтверджує, що навіть технічно достовірні докази можуть бути визнані несумісними зі стандартами справедливого судового розгляду у разі порушення принципів законності, рівності сторін або права на ефективний захист.

Водночас аналіз особливостей фіксації та забезпечення цілісності цифрових доказів свідчить, що технічні методи контролю інформації відіграють важливу, але допоміжну роль у процесі доказування. Використання спеціалізованих засобів копіювання, хешування, документування метаданих та формування ланцюга зберігання дозволяє забезпечити незмінність електронних даних, однак саме по собі не гарантує їх процесуальної допустимості.

Доведено, що ключовою умовою забезпечення доказової сили цифрової інформації є поєднання технічних процедур із чітко визначеною процесуальною формою їх застосування. Відсутність належного документування дій із цифровими доказами, порушення ланцюга їх зберігання або обмеження доступу сторони захисту до інформації створюють ризик втрати доказової цінності електронних даних та можуть призвести до порушення принципів справедливого судового розгляду.

Узагальнюючи результати дослідження, можна констатувати, що ефективне використання цифрових доказів у кримінальному процесі можливе лише за умови інтеграції міжнародних стандартів, технічних механізмів контролю та процесуальних гарантій прав людини. Саме такий комплексний підхід дозволяє забезпечити баланс між потребами кримінального переслідування та необхідністю захисту фундаментальних прав особи в умовах цифровізації правосуддя.

**АНОТАЦІЯ**

У розділі монографії досліджуються теоретико-правові та процесуальні засади забезпечення автентичності й допустимості цифрових доказів у кримінальному процесі в умовах цифровізації суспільних відносин. Проаналізовано правову природу цифрових доказів, їх специфічні ознаки та місце в системі доказового права. Особливу увагу приділено передумовам виникнення проблеми автентичності електронної доказової інформації та чинникам, що ускладнюють її процесуальну оцінку. Розкрито вплив принципів законності, презумпції невинуватості, змагальності сторін і забезпечення права на захист на формування критеріїв допустимості цифрових доказів. Обґрунтовано, що технічна цілісність електронних даних не може розглядатися ізольовано від процесуальної форми їх отримання та дослідження. Зроблено висновок про необхідність формування інтегрованого процесуального підходу до оцінки цифрових доказів, який поєднує технічні та правові механізми з урахуванням стандартів справедливого судового розгляду. Визначено

напрями вдосконалення кримінального процесуального регулювання у сфері використання цифрових доказів.

**Література:**


1. Benedittini and Others v. Italy, № 22152/13, ECHR 2023, § 45–52. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-98442%22]}
2. Convention on Cybercrime (Budapest Convention). Council of Europe, 2001. URL: https://rm.coe.int/1680081561
3. Demirhan v. Turkey, № 13115/21, ECHR 2025 (підтверджено у практиці ЄСПЛ). URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-117601%22]}
4. European Court of Human Rights. Background Paper for the Judicial Seminar 2025. Strasbourg, 2024. URL: https://www.echr.coe.int/documents/d/echr/seminar-background-paper-2025-eng
5. Guidelines on the Treatment of Electronic Evidence in Criminal Proceedings. Commonwealth Secretariat. London, 2025.
6. Information technology -Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012.
7. Kablis v. Russia, № 46118/13, ECHR 2021, § 98. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-192769%22]}
8. Mason S. Electronic Evidence and Electronic Signatures. 5th ed. London: Institute of Advanced Legal Studies, 2021. URL: https://sas-space.sas.ac.uk/9564/1/9781911507246_min.pdf
9. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 27 June 2023 on European Production and Preservation Orders for electronic evidence in criminal matters. *Official Journal of the European Union.* 2023. L 168.
10. ResearchGate. (2025). Electronic evidence in criminal proceedings of Ukraine. URL:https://www.researchgate.net/publication/392347214_Electronic_evidence_in_criminal_proceedings_of_Ukraine
11. *Schatschaschwili v. Germany* [GC], № 30362/08, ECHR 2015, § 101. URL : https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159566%22]}
12. Shyshenko A. A. Digital evidences in criminal proceedings: problems of authenticity and admissibility. *Journal of Law and Social Policy.* 2025. DOI: https://doi.org/10.24144/2788-6018.2025.05.3.46
13. The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations. 2022. SSRN.
14. Алексєєва-Працюк Д. та ін. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. 2018. № 2. С. 247–253 DOI: 10.32842/2078-3736/2025.6.59
15. Антонюк А.Б., Русецька В.А. Електронні докази в кримінальному провадженні // *Міжнародний науковий журнал «Інтернаука»*. 2020. № 10. С. 78–87. DOI: 10.25313/2520-2308-2020-10-6437
16. Гутник Х. М., Хитра О. В. Цифрові докази у кримінальному процесі: монографія. Львів: ЛДУВС України, 2022. 248 с.

17. Гуцалюк М.В., Антонюк П.Є. Щодо сутності електронної (цифрової) інформації як джерел доказів у кримінальному провадженні. *Криміналістичний вісник*. 2020. № 1. С. 37–49.

18. Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та «протидії кібератакам» від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20

19. Квашук О.Д. Використання електронних доказів у кримінальному провадженні. *Центральноукраїнський вісник права та публічного управління.* Випуск/ Issue 2(10), 2025. С. 50–56. DOI https://doi.org/10.32782/cuj-2025-2-5

20. Козицька О.Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2020. № 8. С. 418–421.

21. Конвенція про захист прав людини і основоположних свобод від 04.11.1950// URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

22. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 № 185 (ETS № 185). Ратифікована Законом України № 608-III від 21.09.2005.

23. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

24. Липкан І.І. Особливості доказування у справах про шахрайство, вчинене з використанням цифрових технологій: дис. … д-ра юрид. наук. Київ, 2025. URL: https://dpu.edu.ua/images/Documents/NAUKA/Doktorski%20specializovani%20vceni%20radi/Specializovana%20vcena%20rada%20D%2027.855.03/Lipkan%20Igor%20Ivanovic/Disertacia%20Lipkana%20I.I.pdf

25. Метелев О.П., Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства*. № 1–2, 2023. С. 42–53. DOI: https://doi.org/10.17721/2413-5372.2023.1-2/42-53

26. Метелев О.П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження. *Науковий вісник Ужгородського національного університету*. 2020. № 60. С. 177–181. DOI https://doi.org/10.32782/2307-3322/2020.60.39

27. Метелев О.П. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процес. *Вісник кримінального судочинства*. 2019. № 3. С. 224–238. DOI: https://doi.org/10.17721/2413-5372.2019.3/224-238

28. Мілімко Л.В. Електронні докази в кримінальному судочинстві України. *Науковий вісник УжНУ. Серія «Право».* 2025.

29. Петрик В.В. Використання електронних доказів у кримінальному провадженні. *Науковий вісник Ужгородського Національного Університету. Серія «Право»*. Випуск 87: частина 4. (2025). URL: https://visnyk-jurisuzhnu.com/wp-content/uploads/2025/03/19-3.pdf DOI https://doi.org/10.24144/2307-3322.2025.87.4.17

30. Політова А.С., Чехлай Т.О. Допустимість цифрових доказів у кримінальному провадженні: аналіз судової практики. *Вісник МДУ. Серія: Право*. 2025. № 29. С. 104–115. DOI https://doi.org/10.34079/2226-3047-2025-15-29-104-115

31. Романюк В.В., Абламський С.Є. Критерії допустимості цифрових (електронних) доказів у кримінальному провадженні. *Law and Safety*. 2024. № 2 (93). URL: https://pb.univd.edu.ua/index.php/PB/article/download/818/653 DOI: https://doi.org/10.32631/pb.2024.2.13

32. Сіренко О.В. Електронні докази у кримінальному провадженні. *Міжнародний юридичний вісник*. 2019. № 14. С. 208–214.

33. Стефанів Н. Критерії допустимості й достовірності електронних доказів у кримінальному процесі. *Судова влада України*. 2025. https://supreme.court.gov.ua/supreme/pres-centr/news/1751385/

34. Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України // *Проблеми законності.* 2019. № 146. С. 179–191.

35. Шульга В., Калюжна, Л. Електронні докази у кримінальному процесі: методи їх виявлення, дослідження та правове закріплення. *Теорія та практика судової експертизи і криміналістики*. Вип. 3 (40).2025. С. 136–152. DOI: https://doi.org10.32353/khrife.3.2025.10

**Information about the author:**
**Voloshyna Vladlena Kostyantynivna,**
Candidate of Law, Associate Professor,
Associate Professor of the Department of Criminal Procedure
of the National University "Odesa Law Academy",
23, Fontanska doroga, Odesa, 65009, Ukraine