

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

УДК 343.13:004.738.5

DOI <https://doi.org/10.32782/TNU-2707-0581/2025.2/18>

Антонюк А.О.

Національний юридичний університет імені Ярослава Мудрого

Давиденко С.В.

Національний юридичний університет імені Ярослава Мудрого

ЕЛЕКТРОННІ ДОКАЗИ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ ТА СУДОВОЇ ОЦІНКИ

У презентованій статті досліджуються теоретичні та практичні аспекти використання електронних доказів у кримінальному провадженні. Проаналізовано сучасний стан тематичного правового регулювання крізь призму кримінального процесуального законодавства України та виокремлено проблемні питання збирання, зберігання, дослідження та оцінки даного виду доказової інформації.

Автором систематизовано ключові характеристики електронних доказів, що відрізняють їх від традиційних форм доказів, а саме: нематеріальний характер, необхідність застосування технічних засобів для сприйняття, можливість існування в різних форматах, легкість копіювання та модифікації, наявність метаданих та розподілений характер зберігання. Встановлено, що ці особливості обумовлюють потребу в розробці спеціальних правил та процедур збирання, перевірки, оцінки та зберігання електронних доказів.

У роботі досліджено актуальну судову практику щодо оцінки допустимості електронних доказів, зокрема, правові позиції Верховного Суду стосовно доказів, отриманих з мережі Інтернет, соціальних мереж, електронних пристроїв та використання копій електронних даних.

Розглянуто особливості здійснення міжнародного співробітництва при отриманні електронних доказів у кримінальних провадженнях. Обґрунтовано необхідність удосконалення нормативно-правової бази щодо визначення поняття «електронні докази», критеріїв їх допустимості та оптимального порядку збирання. Сформульовано конкретні пропозиції задля раціоналізації вітчизняного кримінального процесуального законодавства в частині регламентації процедур роботи з електронними доказами та параметрів їх оцінювання. Наголошено на доцільності розробки уніфікованих стандартів фіксації, зберігання та дослідження вказаної доказової інформації з урахуванням її специфічних властивостей.

Результати представлено дослідження мають доктринальне та прикладне значення для вдосконалення процесу доказування в умовах діджиталізації кримінального судочинства України.

Ключові слова: електронні докази, цифрові докази, кримінальне провадження, допустимість доказів, збирання доказів, оцінка доказів, міжнародне співробітництво, кіберзлочинність.

Постановка проблеми. Стрімкий розвиток цифрових технологій та діджиталізація державних механізмів суттєво впливають на всі сфери людської діяльності, включаючи правову.

Сьогодні значна частина інформації створюється, зберігається та передається в електронній формі, що зумовлює нагальну необхідність адаптації правової системи до нових технологічних реалій.

Особливо гостро це питання постає у сфері кримінального судочинства, де від якості та повноти змістовного наповнення різних видів доказів залежить можливість встановлення істини та забезпечення справедливого правосуддя.

Актуальність дослідження порядку використання електронних доказів у кримінальному провадженні обумовлена низкою факторів. По-перше, зростає кількість кримінальних правопорушень, що вчиняються за допомогою електронних пристроїв та мереж, а отже, основні докази таких діянь існують саме в електронній формі. По-друге, традиційна доказова інформація все частіше фіксується завдяки сучасним цифровим технологіям (відеозаписам з камер спостереження, електронним документам, електронним слідам в інформаційних системах тощо). По-третє, чинне кримінальне процесуальне законодавство України не містить достатньо чіткої та детальної регламентації алгоритму роботи з електронними доказами, що створює проблеми у правозастосовній площині.

Аналіз останніх досліджень і публікацій. Аналізуючи доктринальні підходи до визначення поняття електронних доказів, можна виділити декілька основних позицій. Фігурський В.М. розуміє електронні докази як «інформацію, що зберігається в електронному вигляді на будь-яких типах електронних носіїв, в електронних мережах чи хмарних сховищах, а також електронні реквізити, що можуть бути використані для встановлення обставин, що мають значення для кримінального провадження» [3, с. 98]. Отже, дослідник акцентує увагу на формі зберігання інформації та її доказовому значенні.

Марочкін О.І. пропонує розглядати електронні докази як «будь-яку інформацію в цифровій формі, що має значення для кримінального провадження, може бути представлена в матеріалах справи та оцінена судом» [4, с. 24], наголошуючи на цифровій природі інформації та її процесуальному значенні.

У свою чергу, Авдєєва Г. та Живуцька-Козловська Е. вказують на необхідність розмежування понять «електронні докази» та «цифрові докази», зазначаючи, що «цифрові докази є ширшим поняттям, яке охоплює будь-яку доказову інформацію, що зберігається або передається в цифровій формі» [7, с. 127].

Ахтирська Н. та Костюченко О. відмічають, що «правовою основою міжнародного співробітництва у сфері збирання електронних доказів є міжнародні договори та конвенції, а також наці-

ональне законодавство держав» [6, с. 193]. У згаданий спосіб автори наголошують на цінності уніфікації підходів до збирання та оцінки електронних доказів для забезпечення ефективного міжнародного співробітництва у конкретному кримінальному провадженні.

Значну увагу проблемам збирання електронних доказів приділяють Романюк В.В. та Фоміна Т.Г., які досліджують порядок збирання електронних (цифрових) доказів у специфічних категоріях кримінальних проваджень [5].

Постановка завдання. Мета дослідження полягає у визначенні актуального стану та перспектив правового регулювання порядку використання електронних доказів у кримінальному провадженні; аналізі підходів, напрацьованих судовою практикою, до оцінки їх допустимості та формулюванні пропозицій щодо вдосконалення нормативно-правової бази у цій сфері.

Для досягнення поставленої мети необхідно вирішити такі завдання: – з'ясувати наукові позиції щодо визначення поняття «електронний доказ» та його правової природи; – дослідити діюче законодавство України, присвячене регламентації процедур збирання та використання електронних доказів; – проаналізувати судову практику, зокрема, рішення Верховного Суду стосовно оцінки допустимості електронних доказів; – визначити особливості міжнародного співробітництва при отриманні електронних доказів; – сформулювати рекомендації щодо вдосконалення нормативного регулювання правил використання електронних доказів у кримінальному провадженні.

Виклад основного матеріалу. Аналіз чинного кримінального процесуального законодавства України свідчить про відсутність системного підходу до якісного врегулювання питань, пов'язаних з електронними доказами. Так, Кримінальний процесуальний кодекс України (далі – КПК) не містить окремої статті, глави або розділу, присвячених електронним доказам, їх видам, порядку збирання, зберігання та дослідження.

Разом з тим, у різних статтях КПК згадуються окремі види електронної інформації, яка може використовуватися як доказ у кримінальному провадженні. Наприклад, відповідно до ч. 2 ст. 84 КПК, процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів. При цьому електронні докази не виділяються як окреме джерело доказів, а розглядаються в рамках таких категорій, як «речові докази» та «документи».

Так, у ч. 1 ст. 98 КПК вказується, що речовими доказами є матеріальні об'єкти, які були знаряддям вчинення кримінального правопорушення, зберегли на собі його сліди або містять інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. Згідно з ч. 2 ст. 98 КПК документи є речовими доказами, якщо вони містять ознаки, зазначені в ч. 1 цієї статті.

Стаття 99 КПК визначає поняття документа як джерела доказів, під яким розуміють спеціально створений з метою збереження інформації матеріальний об'єкт, котрий містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження (ч. 1). Частина 2 ст. 99 КПК уточнює, що до документів, за умови наявності в них відомостей, передбачених ч. 1 цієї статті, можуть належати: 1) матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації, зокрема, електронні (у тому числі комп'ютерні дані); 2) матеріали, отримані внаслідок здійснення під час кримінального провадження заходів, передбачених чинними міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України; 3) складені в порядку, передбаченому цим Кодексом, протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії; 4) висновки ревізій та акти перевірок; 5) довідки, висновки та інші документи спеціалістів [1].

Таким чином, електронні носії інформації розглядаються законодавцем як різновид документів, що може бути процесуальним джерелом доказів у кримінальному провадженні. Водночас, КПК України не містить спеціальних правил щодо порядку збирання, зберігання та дослідження електронних доказів, які б враховували їх характерологічні ознаки.

Окремі аспекти роботи з електронними доказами регламентуються в контексті проведення негласних слідчих (розшукових) дій. Наприклад, ст. 264 КПК передбачає можливість зняття інформації з електронних інформаційних систем без відома їх власника, володільця або утримувача. Статтею 265 КПК унормовані процедури фіксації та збереження інформації, отриманої з комунікаційних мереж за допомогою технічних засобів, а також інших даних.

Крім того, деякі питання, пов'язані з електронними доказами, врегульовані спеціальними

нормативно-правовими актами. Зокрема, Закон України «Про електронні документи та електронний документообіг» визначає поняття електронного документа та його юридичну силу [7]. Закон України «Про електронні довірчі послуги» регламентує відносини у сферах надання електронних довірчих послуг та електронної ідентифікації [8].

На відміну від кримінального процесуального законодавства, Цивільний процесуальний кодекс України, Господарський процесуальний кодекс України та Кодекс адміністративного судочинства України закріплюють дефініцію електронних доказів. Так, відповідно до ч. 1 ст. 100 ЦПК, електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, які мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі [10].

Водночас, аналіз чинного тематичного законодавства свідчить про відсутність системного підходу до регулювання питань, присвячених електронним доказам в кримінальному провадженні. Це створює низку проблем у правозастосовній практиці – при алгоритмізації порядку збирання, фіксації, зберігання, дослідження, використання електронних доказів, а також напрацюванні єдиних критеріїв їх допустимості та достовірності.

Спробою правової раціоналізації цього сегменту був проєкт Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» від 01.09.2020 № 4004 [2]. У документі пропонувалося визначити електронні докази як «інформацію в електронній (цифровій) формі з відомостями, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження». Втім, названий законопроект не був прийнятий, що залишило відкритим питання необхідності нормативного формування категорії «електронні докази».

На нашу думку, електронними доказами в кримінальному провадженні слід вважати фактичні дані, зафіксовані в електронній (цифровій) формі або на відповідних носіях інформації, містять відомості про обставини, що мають значення для кримінального провадження, та отримані в порядку, передбаченому кримінальним процесуальним законодавством.

Підкреслимо: електронні докази характеризує низка специфічних властивостей, які відрізняють їх від традиційних доказів:

1. Нематеріальний характер – електронні докази існують у вигляді інформації, записаної у формі двійкового коду, що робить неможливим їх безпосереднє сприйняття без використання спеціальних технічних засобів.

2. Необхідність застосування релевантних програмно-технічних засобів для сприйняття – для гарантування можливості сприйняття та розуміння змісту електронного доказу, використовується відповідне апаратне та програмне забезпечення.

3. Можливість існування доказів у різних формах – одна і та сама інформація може бути представлена у текстовому, графічному, аудіо-, відеоформаті й ін., що ускладнює її ідентифікацію та дослідження.

4. Легкість копіювання та модифікації – електронні докази можуть бути вільно скопійовані, змінені або знищені без залишення явних / очевидних слідів, що створює труднощі при забезпеченні їх автентичності та цілісності.

5. Наявність метаданих – електронні докази містять не лише основну інформацію, а й так звані «метадані» (інформацію про інформацію), які можуть мати суттєве значення для встановлення фактів, обставин провадження.

6. Розподілений характер зберігання – електронні докази можуть зберігатися на різних пристроях та серверах, розташованих у відмінних географічних локаціях, що значно ускладнює їх збирання та фіксацію.

Вбачається, що зазначені властивості електронних доказів обумовлюють необхідність розробки спеціальних правил та процедур їх збирання, перевірки, оцінки та зберігання, котрі враховували б їх полікомпонентну специфіку.

Аналіз актуальної судової практики дозволяє виявити популярні тенденції та підходи до оцінки допустимості електронних доказів у кримінальному провадженні. Так, Верховний Суд у своїх рішеннях формулює правові позиції, що заповнюють прогалини у законодавчому регулюванні порядку використання даного виду доказової інформації.

Наприклад, у постанові об'єднаної палати Касаційного кримінального суду у складі Верховного Суду від 29 березня 2021 р. (справа № 554/5090/16-к) сформовано позицію щодо допустимості електронних доказів, отриманих з мережі Інтернет (з відкритих джерел). Зокрема, Суд зазна-

чив, що «інформація, отримана з мережі Інтернет, може бути використана як доказ у кримінальному провадженні за умови дотримання процедури її збирання та фіксації, яка забезпечує можливість її перевірки» [11].

Постановою колегії суддів Першої судової палати Касаційного кримінального суду у складі Верховного Суду від 21 вересня 2023 р. (справа № 392/569/18) окреслено питання допустимості електронних доказів, одержаних під час обшуку електронних пристроїв. Суд наголосив на необхідності «детального опису електронних носіїв інформації у протоколі обшуку та гарантування їх належного зберігання для забезпечення допустимості отриманих доказів» [12], що орієнтує на важливість організаційних аспектів роботи з ними.

Істотне значення у презентованому контексті має постанова колегії суддів Першої судової палати Касаційного кримінального суду у складі Верховного Суду від 26 січня 2021 р. (справа № 236/4268/18), в якій розглянуто проблему оцінки електронних доказів, одержаних із соціальних мереж. Верховний Суд відзначив, що «скріншоти сторінок соціальних мереж можуть бути визнані допустимими доказами за умови, що вони отримані в порядку, передбаченому КПК України, та їх автентичність може бути підтверджена» [13]. Отже, дана позиція визначає критерії допустимості специфічного виду електронних доказів.

Особливу увагу привертає практика Верховного Суду щодо допустимості електронних доказів за 2023 р. Як декларується на офіційному сайті Верховного Суду, у цей період було сформовано вагому правову позицію щодо використання їх копій: «копії електронних даних можуть бути визнані допустимими доказами, однак, у разі заяви сторони про фальсифікацію такої копії, суд може вилучити оригінал» [20]. Процитоване рішення має надважливе значення для практики правозастосування, оскільки встановлює баланс між процесуальною економією та необхідністю перевірки достовірності електронних доказів.

Наведені «настанови» щодо правильності оцінки електронних доказів є пріоритетними для вироблення єдиної та сталої практики використання електронних доказів у кримінальному провадженні. Разом із тим, як вказує Потапов І.Ф., «для забезпечення правової визначеності необхідно закріпити критерії допустимості електронних доказів на законодавчому рівні» [14, с. 125].

Продовжуючи міркування у заданому напрямі, нагадаємо, що інститут міжнародного співро-

бітництва відіграє магістральну роль у збиранні електронних доказів, особливо під час здійснення кримінальних проваджень, пов'язаних з кіберзлочинністю та транснаціональними злочинами. Означене зумовлено глобальним характером інформаційних технологій та можливістю зберігання електронних доказів на серверах, розташованих в різних країнах.

Ахтирська Н. та Костюченко О. відмічають, що «правовою основою міжнародного співробітництва у сфері збирання електронних доказів є міжнародні договори та конвенції, а також національне законодавство держав» [6, с. 193]. У згаданий спосіб автори наголошують на цінності уніфікації підходів до збирання та оцінки електронних доказів для забезпечення ефективного міжнародного співробітництва у конкретному кримінальному провадженні.

Як підкреслює Ангеленюк А.-М.Ю., «важливим аспектом міжнародного співробітництва у сфері збирання електронних доказів є забезпечення оперативності надання правової допомоги, що особливо актуально, з огляду на швидкоплинний характер електронної інформації» [15]. Авторка наголошує на необхідності розробки спеціальних механізмів прискореного надання правової допомоги у випадках, коли існує ризик втрати електронних доказів.

Вивчення міжнародного досвіду правової регламентації правил використання електронних доказів у кримінальному судочинстві має неocenне значення для якісного вдосконалення діючого вітчизняного законодавства та новочасної правозастосовної дійсності у цій сфері. Відповідно аналіз тематично орієнтованих доктрин, нормативних актів та практики компетентних суб'єктів іноземних держав дозволяє виявити найбільш продуктивні шляхи вирішення прикладних проблем, пов'язаних з електронними доказами.

Так, Московчук Д.О. у компаративному дослідженні електронних доказів зазначає, що «в країнах загального права (США, Велика Британія) електронні докази регулюються більш детально, з чіткими процесуальними нормами щодо їх збирання, зберігання та оцінки, тоді як країни континентального права поступово адаптують своє законодавство до вимог цифрової епохи» [21, с. 87]. При цьому виділяється позитивний досвід Німеччини, де прийнято спеціальні інструкції для прокурорів та слідчих щодо роботи з електронними доказами, які мають рекомендаційний характер, але широко застосовуються на практиці.

Разом з тим, одним із генеральних міжнародних документів у секторі протидії злочинності у кіберпросторі є Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) 2001 р. [16], котра містить низку положень, присвячених процедурам збирання, зберігання та обміну електронними доказами між державами-учасницями.

У США правова регламентація електронних доказів здійснюється на підставі Федеральних правил про докази (Federal Rules of Evidence), які закріплюють спеціальні приписи щодо допустимості електронних доказів. Зокрема, Правило 901(b)(4) передбачає можливість автентифікації електронних доказів на основі їх «зовнішнього вигляду, змісту, внутрішніх шаблонів або інших відмінних характеристик, взятих разом з обставинами» [17]. Крім того, у США діють керівництва для правоохоронних органів щодо збирання та дослідження електронних доказів, розроблені Національним інститутом стандартів та технологій (NIST) та Федеральним бюро розслідувань (FBI).

У Великій Британії провідним нормативним актом, який регулює питання електронних доказів, є Закон про поліцію та докази у кримінальних справах 1984 р. (Police and Criminal Evidence Act 1984, PACE) [18]. Згідно з названою легітимністю, електронні докази визнаються допустимими у кримінальному провадженні, якщо вони є релевантними для справи та автентичними. Для забезпечення автентичності електронних доказів застосовується «ланцюг зберігання» (chain of custody), котрий передбачає документування всіх дій з електронними доказами від моменту їх вилучення до представлення в суді.

Практика міжнародного співробітництва у процедурі збирання електронних доказів демонструє певні особливості та складнощі, які необхідно враховувати при розробці вітчизняної нормативно-правової бази у цій галузі.

Ахтирська Н. та Костюченко О. виділяють такі основні форми міжнародного співробітництва при збиранні електронних доказів: «запити про правову допомогу, створення спільних слідчих груп, обмін інформацією між правоохоронними органами різних держав, співпраця з міжнародними організаціями» [6, с. 195]. Кожна з цих форм має власну специфіку та процедури, яких слід дотримуватися для забезпечення допустимості отриманих доказів.

Помітну роль у сфері міжнародного співробітництва при збиранні електронних доказів відіграють міжнародні організації та мережі (Інтерпол,

Європол, Євроюст та ін.). Вони надають технічну та організаційну підтримку правоохоронним органам різних держав при розслідуванні транснаціональних злочинів, пов'язаних з використанням інформаційних технологій [7, с. 129].

Однак, як позначає Ангеленюк А.-М.Ю., «міжнародне співробітництво при збиранні електронних доказів стикається з певними труднощами, зокрема, різницею в правових системах різних держав, відсутністю уніфікованих стандартів роботи з електронними доказами, мовними та технологічними бар'єрами» [15, с. 200]. Це, своєю чергою, зумовлює нагальну потребу створення міжнародних стандартів та протоколів роботи із вказаним видом доказів.

Важливим кроком за даним вектором діяльності є впровадження «Протоколу Берклі з ведення розслідувань з використанням відкритих цифрових даних» [19]. Документ містить чіткі рекомендації щодо збирання, збереження й аналізу цифрових доказів, отриманих з відкритих джерел, та може бути застосований як орієнтир при розробці національних моделей цих процедур.

Крім того, у багатьох країнах системно напрацьовані прикладні методичні рекомендації та стандарти для правоохоронних органів щодо роботи з електронними доказами, які не мають юридичної сили законодавчих актів.

Висновки. Пізнання європейського / міжнародного досвіду [21, 22] дозволяє: (1) зробити висновок про доцільність втілення комплексного підходу до правового регулювання алгоритму використання електронних доказів у кримінальному провадженні, який би оптимально поєдну-

вав нормативне закріплення основних термінологічних конструкцій та процедур з розробленням деталізованих методичних порадників, довідників тощо для практичних працівників; (2) сформулювати конкретні пропозиції, спрямовані на вдосконалення чинного процесуального законодавства України в аспекті запровадження:

- сучасних нормативних дефініцій та відповідних стандартів, протоколів (за прикладом США);
- концепції «ланцюг збереження доказів» (на кшталт британської моделі), що передбачає послідовну документацію всіх операцій, проведених з електронними доказами від моменту їх виявлення до презентації в суді;
- процедури сертифікації програмного забезпечення, яке застосовується для збирання та аналізу електронних доказів, що, безумовно, підвищить ступінь їх надійності, достовірності та допустимості (на основі німецького досвіду);
- інтегрованих інформаційних систем, які автоматизують процес збирання, зберігання та обміну електронними доказами між різними суб'єктами кримінальних процесуальних відносин (за зразком естонської системи);
- механізму «швидкого заморожування» електронних даних (згідно з вимогами Будапештської конвенції) для запобігання знищенню чи модифікації вирішальних електронних доказів до отримання дозволу суду на їх вилучення.

Введення запропонованих змін сприятиме підвищенню рівня ефективності регламенту використання електронних доказів у кримінальному провадженні України та гарантуватиме їх відповідність міжнародним стандартам.

Список літератури:

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (дата звернення: 06.03.2025).
2. Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів : Проект Закону України від 01.09.2020 № 4004. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771 (дата звернення: 07.03.2025).
3. Фігурський В. М. Докази в електронній формі у кримінальному провадженні. *Галицькі студії: Юридичні науки*. 2023. № 4. С. 97–105.
4. Марочкін О. І. Особливості використання електронних доказів у кримінальному провадженні. *Альманах наукових праць фахівців НДІ ВПЗ*. 2022. С. 24–30.
5. Романюк В. В., Фоміна Т. Г. Порядок збирання електронних (цифрових) доказів у кримінальних провадженнях про колабораційну діяльність. *Вісник Кримінологічної асоціації України*. 2024. Т. 32. № 2. С. 344–353.
6. Ахтирська Н., Костюченко О. Процесуальні та організаційні аспекти збору електронних доказів під час міжнародного співробітництва. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2022. Т. 2. № 72. С. 192–198.
7. Авдєєва Галина, Ельжбета Живуцька-Козловська. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика судової експертизи і криміналістики*. 2023. С. 126–143.

8. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text> (дата звернення: 10.03.2025).
9. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text> (дата звернення: 10.03.2025).
10. Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV. URL: <https://zakon.rada.gov.ua/laws/show/1618-15#Text> (дата звернення: 10.03.2025).
11. Постанова об'єднаної палати Касаційного кримінального суду Верховного Суду від 29 березня 2021 року у справі № 554/5090/16-к (провадження № 51-1878км20). URL: <https://reyestr.court.gov.ua/Review/96074938> (дата звернення: 12.03.2025).
12. Постанова колегії суддів Першої судової палати Касаційного кримінального суду Верховного Суду від 21 вересня 2023 року у справі № 392/569/18 (провадження № 51-1877км23). URL: <https://reyestr.court.gov.ua/Review/113794565> (дата звернення: 12.03.2025).
13. Постанова колегії суддів Першої судової палати Касаційного кримінального суду Верховного Суду від 26 січня 2021 року у справі № 236/4268/18 (провадження № 51-3124км20). URL: <https://reyestr.court.gov.ua/Review/94905297> (дата звернення: 12.03.2025).
14. Потапов І. Ф. Здійснення кримінального провадження в умовах воєнного стану: практика ЄСПЛ та Верховного Суду. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. С. 124–130.
15. Ангеленюк А.-М. Ю. Взаємодія правоохоронних органів у межах міжнародного співробітництва під час збирання електронних доказів учинення злочину. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Вип. 81. Ч. 3. С. 9–13.
16. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 06.03.2025).
17. Federal Rules of Evidence. URL: <https://www.law.cornell.edu/rules/fre> (дата звернення: 05.02.2025).
18. Police and Criminal Evidence Act 1984. URL: <https://www.legislation.gov.uk/ukpga/1984/60/contents> (дата звернення: 27.03.2025).
19. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних / Управління Верховного комісара ООН з прав людини та Центру з прав людини Каліфорнійського університету в Берклі. Юридична школа, 2020. 119 с. URL: <https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf> (дата звернення: 14.03.2025).
20. Верховний Суд: копії електронних даних можуть бути визнані допустимими доказами. Офіційний сайт Верховного Суду. URL: <https://supreme.court.gov.ua/supreme/pres-centr/news/1751385/> (дата звернення: 15.03.2025).
21. Московчук Д. О. Електронні докази у країнах континентального та загального права: порівняльно-правове дослідження : дис. ... канд. юрид. наук : 12.00.09. Одеса, 2023.
22. Антонюк О. Електронне кримінальне провадження: міжнародний досвід використання інформаційних систем алгоритмізації кримінальної юстиції. *Науковий вісник Дніпровського державного університету в внутрішніх справах*. 2024. № 1. С. 253–263.

Antoniuk A.O., Davydenko S.V. ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS: PROSPECTS FOR LEGAL REGULATION AND JUDICIAL EVALUATION

This article examines the theoretical and practical aspects of using electronic evidence in criminal proceedings. The current state of thematic legal regulation is analyzed through the lens of Ukrainian criminal procedural legislation, and problematic issues of collection, storage, examination, and evaluation of this type of evidentiary information are identified.

The research systematizes the key characteristics of electronic evidence that distinguish it from traditional forms of evidence, specifically: intangible nature, the need for technical means for perception, the possibility of existing in different formats, ease of copying and modification, presence of metadata, and distributed storage nature. It has been established that these features necessitate the development of special rules and procedures for collecting, verifying, evaluating, and storing electronic evidence.

The paper examines current judicial practice regarding the assessment of the admissibility of electronic evidence, in particular, the legal positions of the Supreme Court concerning evidence obtained from the Internet, social networks, electronic devices, and the use of copies of electronic data. The author analyzes landmark Supreme Court decisions that have shaped the approach to electronic evidence admissibility, including decisions from 2021-2023 that established important precedents for practitioners.

The features of international cooperation in obtaining electronic evidence in criminal proceedings are considered. The necessity of improving the regulatory framework regarding the definition of «electronic

evidence,» criteria for its admissibility, and optimal collection procedures is substantiated. The author examines various forms of international cooperation, including legal assistance requests, joint investigation teams, information exchange between law enforcement agencies of different countries, and cooperation with international organizations. The significant role of international organizations (Interpol, Europol, Eurojust) in providing technical and organizational support to law enforcement agencies investigating transnational crimes related to information technologies is highlighted.

The article also presents a comparative analysis of approaches to regulating electronic evidence in various legal systems, including common law countries (USA, Great Britain) and continental law countries, with particular attention to positive experiences that could be implemented in Ukrainian legislation. The author emphasizes that while common law countries have more detailed procedural rules for the collection, storage, and evaluation of electronic evidence, continental law countries are gradually adapting their legislation to the requirements of the digital era.

Specific proposals have been formulated to rationalize domestic criminal procedural legislation regarding the regulation of procedures for working with electronic evidence and parameters for its evaluation. These include the introduction of modern regulatory definitions and standards, the concept of «chain of preservation of evidence,» certification procedures for software used to collect and analyze electronic evidence, integrated information systems that automate the process of collecting, storing, and exchanging electronic evidence, and mechanisms for «quick freezing» of electronic data.

The necessity of developing unified standards for recording, storing, and examining the specified evidentiary information, taking into account its specific properties, is emphasized. The implementation of the proposed changes would increase the effectiveness of regulations for using electronic evidence in criminal proceedings in Ukraine and ensure their compliance with international standards.

The results of the presented research have doctrinal and applied significance for improving the process of proof in the conditions of digitalization of criminal justice in Ukraine.

Key words: *electronic evidence, digital evidence, criminal proceedings, admissibility of evidence, collection of evidence, evaluation of evidence, international cooperation, cybercrime.*