



УДК 343.1

DOI <https://doi.org/10.32782/cuj-2025-2-5>**Квашук Олександр Дмитрович**

кандидат юридичних наук, старший викладач кафедри кримінального процесу та криміналістики факультету № 1 Донецького державного університету внутрішніх справ
ORCID: 0009-0008-5969-4576

ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

У статті досліджено правову природу, процесуальні особливості та практичні аспекти використання електронних доказів у кримінальному провадженні України. Актуальність теми зумовлена стрімким розвитком цифрових технологій, поширенням кіберзлочинності та необхідністю адаптації національного законодавства до сучасних викликів у сфері кримінального судочинства. Автор аналізує основні види електронних доказів, зокрема електронні документи, мультимедійні файли, метадані, інформацію із соціальних мереж і цифрові сліди із серверів та пристроїв. Розглянуто специфіку їх збирання, фіксації, зберігання та оцінки з урахуванням вимог Кримінального процесуального кодексу України, а також міжнародних стандартів.

Особлива увага приділяється проблемам допустимості електронних доказів, таким як недотримання процедур вилучення, автентифікація, захист від фальсифікації та дотримання прав особи під час обшуку цифрових носіїв. Проаналізовано судову практику, яка демонструє неоднорідність у підходах до оцінки цифрових доказів, що вказує на необхідність уніфікації відповідних процесуальних норм. Окреслено роль судових експертів у встановленні технічної достовірності та автентичності електронних даних, надано приклади справ, де саме експертиза відіграла вирішальну роль.

У статті також узагальнено зарубіжний досвід правового регулювання електронних доказів (США, ЄС, Велика Британія) з метою формування пропозицій щодо вдосконалення вітчизняного кримінального процесу. Автор підкреслює необхідність нормативного закріплення поняття «електронний доказ», розробки методичних рекомендацій для слідчих і суддів, а також впровадження цифрової криміналістики в українську судову практику. Зроблено висновок, що ефективне правове врегулювання використання електронних доказів є ключовою умовою забезпечення об'єктивності, законності та справедливості кримінального провадження у цифрову епоху.

Ключові слова: електронні докази, кримінальне провадження, допустимість доказів, кримінальне провадження.

Kvashuk O. D. The use of electronic evidence in criminal proceedings

The article examines the legal nature, procedural features and practical aspects of the use of electronic evidence in criminal proceedings in Ukraine. The relevance of the topic is due to the rapid development of digital technologies, the spread of cybercrime and the need to adapt national legislation to modern challenges in the field of criminal justice. The author analyzes the main types of electronic evidence – in particular, electronic documents, multimedia files, metadata, information from social networks and digital traces from servers and devices. The specifics of their collection, recording, storage and evaluation are considered, taking into account the requirements of the Criminal Procedure Code of Ukraine, as well as international standards.

Particular attention is paid to the problems of admissibility of electronic evidence, such as non-compliance with the procedures for seizure, authentication, protection against falsification and observance of the rights of the individual during the search of digital media. The case law is analyzed, which demonstrates heterogeneity in approaches to the assessment of digital evidence, which indicates the need to unify the relevant procedural norms. The role of forensic experts in establishing the technical reliability and authenticity of electronic data is outlined, and examples of cases where expertise played a decisive role are provided.

The article also summarizes foreign experience in legal regulation of electronic evidence (USA, EU, Great Britain), in order to formulate proposals for improving the domestic criminal process. The author emphasizes

the need for regulatory consolidation of the concept of “electronic evidence”, the development of methodological recommendations for investigators and judges, as well as the introduction of digital forensics into Ukrainian judicial practice. The conclusion is made that effective legal regulation of the use of electronic evidence is a key condition for ensuring the objectivity, legality and fairness of criminal proceedings in the digital era.

Key words: *electronic evidence, criminal proceedings, admissibility of evidence, criminal proceedings.*

Вступ. У контексті цифрової трансформації сучасного суспільства інформаційні технології набувають дедалі більшого значення у всіх сферах життя, зокрема й у кримінальному судочинстві. У зв'язку з цим особливої актуальності набуває питання використання електронних доказів у кримінальному провадженні. Електронні докази мають специфічні риси, що потребують адаптації наявних правових норм, а також впровадження нових механізмів забезпечення їх допустимості, достовірності та цілісності.

Матеріали та методи. Електронні докази у кримінальному процесі досліджували М. Гуцалюк, І. Каланча, О. Сіренко, А. Скрипник, А. Столітній, В. Хахановський та інші. Однак із врахуванням динаміки розвитку інноваційних технологій, зокрема у сфері електроніки, необхідно надалі детально та постійно вивчати використання електронних доказів у кримінальному процесі України.

Методологічною основою дослідження є сукупність методів та прийомів наукового пізнання, що включає теоретичні та емпіричні загальнонаукові методи (аналізу, синтезу, абстрагування, аналогії, структурно-функціональний та інші), які дозволили всебічно вивчити проблему, а також спеціальні методи (формально-юридичний, порівняльно-правовий, метод аналізу й узагальнення судової практики), що забезпечили глибину та точність проведеного аналізу.

Результати. Відповідно до ст. 84 КПК України доказами є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів, а у провадженнях щодо кримінальних проступків – також пояснення

осіб, результати медичного освідчення, висновок спеціаліста, показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису (ч. 2 ст. 84, ст. 298-1 КПК України) [1].

Відповідно до ч. 1 ст. 99 КПК України документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який 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. А в ч. 2 цієї статті зазначено, що до документів, за умови наявності в них відомостей, передбачених частиною першою, можуть належати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані) [1].

Електронні докази в кримінальному процесі України набувають дедалі більшої актуальності, що вимагає глибокого осмислення та належного правового регулювання. У випадку, коли такі докази оформлені неналежним чином, є ризик визнання їх недопустимими, що унеможливить їх врахування судом під час ухвалення рішення у кримінальному провадженні.

Слід підкреслити, що стрімке зростання використання електронних доказів зумовлене активним проникненням цифрових технологій в усі сфери життя. На відміну від минулих десятиліть, нині майже кожна особа має доступ до мобільних телефонів із розширеним функціоналом. Як наслідок, значна частина доказової інформації одразу фіксується у цифровому форматі. Поширеною практикою стало надання свідками відеозаписів кримінальних подій, збережених у пам'яті їхніх мобільних пристроїв, що безпосередньо залучається до матеріалів кримінального провадження.

Електронні докази – це інформація в електронній (цифровій) формі, яка зберігається, обробляється або передається за допомогою електронних пристроїв та може бути використана як доказ у кримінальному провадженні. До них належать електронні листи, текстові повідомлення, файли, записи камер відеоспостереження, метадані, інформація з вебсайтів, соціальних мереж тощо.

Цифрові сліди, які залишаються унаслідок використання інформаційно-комунікаційних технологій користувачами, можуть розкрити відомості про них, що зберігаються в цифрових пристроях (наприклад, комп'ютерах та планшетах, телефонах, принтерах, «розумних» телевізорах і будь-яких інших пристроях, зовнішніх запам'ятовуючих пристроях (наприклад, зовнішніх жорстких дисках і USB – флеш-накопичувачах, мережових компонентах і пристроях (наприклад, маршрутизаторах), серверах і хмарному середовищі. Дані, що добуваються, можуть бути ідентифіковані як контент (тобто слова в письмових повідомленнях або вимовлені слова в аудіо-файлі, наприклад, відео, текст електронних листів, текстові повідомлення, миттєві повідомлення та зміст соціальних мереж), і дані, що не відносяться до контенту, або метадані (тобто дані про зміст, наприклад, особистість і місце розташування користувачів, і дані про операції, такі як інформація про відправників і одержувачів) [2, с. 178].

Прийняття Закону 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 березня 2022 року № 2137-IX [3] стало важливим кроком у регламентації використання електронних доказів. Однак певна кількість питань залишається невирішеною у правовому полі. З метою привернення уваги законодавця до проблемних питань використання електронних доказів у кримінальному процесуальному праві України слід розглянути окремі з них та надати пропозиції щодо шляхів їх можливого вирішення.

У науці відсутнє єдине розуміння місця електронних доказів у системі процесуальних джерел доказів: висловлюються аргументи як на користь віднесення їх до традиційних (речові докази, документи), так і на користь виділення окремої групи (цифрові чи електронні докази).

Наразі електронні докази часто вважають речовими чи доказами-документами, що не охоплює їхню природу (не мають матеріального носія, легко змінюються), а недостатня правова визначеність у питанні процесуальної природи відповідних джерел зумовлює труднощі в їх процесуальній кваліфікації. Так, у судовій практиці є випадки визнання судом електронними доказами файлів, а речовими доказами – носіїв, на яких вони знаходяться. У інших випадках суд розглядає електронні докази як електронні документи [4, с. 96], хоча обсяг поняття електронного документа є вужчим за поняття електронного доказу. Так, електронний документ повинен містити обов'язкові реквізити, які притаманні документам. Своєю чергою електронний доказ не завжди має такі реквізити, однак містить відомості про доказові факти або обставини, що підлягають доказуванню.

З огляду на правову природу електронного доказу доречно було б закріпити визначення електронного доказу в КПК України (в новій статті 99-1 КПК). Запропонована норма: «Електронний доказ – це будь-яка інформація в цифровій формі, яка створена, збережена або передана з використанням комп'ютерних технологій, мереж або пристроїв, що містить відомості про обставини, що підлягають доказуванню в кримінальному провадженні».

Судова практика в Україні щодо електронних доказів показує, що вітчизняні суди все ще стикаються з низкою проблем, пов'язаних з допустимістю та оцінкою електронних доказів. Зокрема, суди інколи відмовляються приймати докази через неналежне дотримання процесуальних вимог під час їх збору або перевірки [5, с. 25]. Це підкреслює важливість вдосконалення правових норм та підвищення підготовки фахівців у цій сфері.

З розвитком технічних засобів і нових нормативно-правових актів ситуація посту-

пово покращується, але досягнення належного рівня ефективності в цій сфері потребує часу [6, с. 16].

Звернемо увагу на Постанову Верховного Суду від 13.07.2020 у справі № 753/10840/19, в якій судами було зроблено два висновки, а саме: висловлення погроз з боку колишнього чоловіка за допомогою Viber є психологічним насильством, а скріншоти з мобільних пристроїв можуть бути належним доказом вчинення такого насильства. Під час розгляду справи представником відповідача наголошувалося, що надані заявником роздруківки містять лише імена людей, у тому числі кривдника як відправника, проте не надано доказів, з якого саме мобільного номера та на які номери надсилались ці повідомлення, що унеможливило встановлення відправника та адресата, а тому не можуть бути належними та допустимими доказами відправлення цих повідомлень саме відповідачем. Однак Касаційний цивільний суд із такими доводами не погодився та визнав скріншоти електронної переписки у застосунку Viber належними доказами психологічного насильства з боку відповідача [7].

Важлива у питанні забезпечення єдності правозастосування позиція Верховного Суду наведена у справі № 751/6069/19. З матеріалів провадження видається, що наявний у справі DVD-R-диск з відеозаписом обставин події з камер відеоспостереження був добровільно наданий директором ТОВ «Р» на запит слідчого, а отже, необхідності звертатися з відповідним клопотанням до слідчого судді для отримання копії цього запису в останнього не було. Верховний Суд підкреслив, що долучений слідчим до матеріалів провадження в якості речового доказу DVD-R-диск з відеозаписом обставин події був виготовлений у зв'язку із необхідністю надання інформації, яка має значення у кримінальному провадженні, та є самостійним джерелом доказу, похідним від інформації, що зберігається на комп'ютері в електронному вигляді у вигляді файлів. Отже, записаний на оптичний диск – носій інформації, електронний файл у вигляді відеозапису є оригіналом (відображенням) електронного документа [8].

Потреба вдосконалення нормативної регламентації актуалізує всебічне дослідження іноземного досвіду ефективності підходів, засобів і методів роботи з електронними доказами.

У США активно застосовуються методи цифрової криміналістики для збору і аналізу даних з мобільних телефонів та комп'ютерних пристроїв, що дозволяє ефективно боротися з кіберзлочинністю [9, с. 47].

Комітет безпеки Європейського Союзу визначає електронні докази як дані, що зберігаються в електронному вигляді, наприклад, IP-адреси, електронні листи, фотографії або імена користувачів, які мають значення для кримінального процесу. Зазвичай такі дані знаходяться у постачальників послуг, а правоохоронні та судові органи змушені звертатися до них для отримання необхідної інформації. У національному законодавстві Австрії, Болгарії, Чеської Республіки, Італії, Швеції та інших держав офіційне визначення електронних доказів відсутнє. Законодавство Португалії також не містить визначення терміна «електронний доказ», однак у цій країні використовується наукове визначення, згідно з яким електронний доказ – це будь-який тип інформації, що має доказове значення та зберігається на цифровому пристрої або передається в цифровій чи двійковій формі [10, с. 169].

Німеччина, Бельгія, Іспанія, Фінляндія, Франція, Ірландія, Італія, Люксембург, Португалія та Румунія визнають електронні документи рівнозначними паперовим документам та надають їм юридичне значення у судовому процесі [11, с. 286].

В Україні ж, хоча нормативно-правова база щодо електронних доказів поступово вдосконалюється, необхідно ще чітко унормувати деякі аспекти цього процесу, впроваджуючи досвід інших країн.

Ю.Ю. Орлов та С.С. Чернявський стверджують, що умови допустимості до «класичного» документа як джерела доказів є такими ж, як і до електронних відображень, що їх сформувала людина:

1) має бути відомим автор документа (установа, організація, підприємство, посадова особа або громадянин);

2) зміст документа має відповідати компетенції і фактичній обізнаності автора.

Саме це і дозволяє перевірити доказ. Проте, на їхню думку, ті електронні відображення, що створені інформаційною системою в автоматичному режимі, вимогу про відомість автора як умову допустимості доказу висувати не слід. Разом із тим у деяких випадках може виявитися необхідним призначити комп'ютерно-технічну експертизу щодо визначення можливості формування певного електронного відображення конкретним апаратно-програмним комплексом з метою встановлення належності доказу [12, с. 120].

Цей підхід є логічним і прогресивним, враховує специфіку цифрового середовища, у якому події (логін, геолокація, час доступу тощо) часто фіксуються без участі людини. Але наполягати на «авторстві» там, де його не існує в класичному розумінні, помилково й технічно неможливо, тому ця модель потребує посиленої уваги до достовірності автоматичних даних – саме тут комп'ютерно-технічна експертиза має велике значення.

Засоби і методи техніко-криміналістичного дослідження цифрових доказів характеризуються широким інструментарієм, як комерційним, так і з відкритим кодом. Ця галузь має свій міжнародний стандарт, який був імплементований і в Україні – ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT)» [13, с. 288].

Досить слушно зауважив Д.М. Цехан, що задля забезпечення допустимості «цифрових доказів» необхідно використовувати можливості сучасних судових техніко-криміналістичних експертиз, зокрема: експертизи комп'ютерної техніки і програмних продуктів, інформаційно-комп'ютерної експертизи та комплексної експертизи. При цьому увага експерта має зосереджуватись на виявленні ознак модифікації цифрової інформації, її способів та меж [14, с. 259]. Ця позиція є практико-орієнтованою і цілком виправданою. В умовах, коли цифрові файли легко редагуються, метадані можуть бути змінені або підроблені, доказова інформація збе-

рігається на хмарних сервісах за межами України.

Роль експерта полягає не лише у встановленні автентичності, але і у викритті потенційних маніпуляцій, що своєю чергою посилює надійність електронних доказів, що використовуються у доказуванні.

Специфіці об'єктів та вирішуваних завдань відповідного експертного дослідження найбільше відповідає назва «цифрова криміналістична експертиза», яку доцільно запровадити. У відповідних інструкціях щодо призначення та проведення судових експертиз доцільно конкретизувати завдання судової цифрової експертизи (хеш-ідентифікація, відновлення видалених файлів, встановлення авторства електронного документа та внесення змін до баз даних тощо), об'єкти та орієнтовний перелік вирішуваних питань.

Наведені пропозиції покликані забезпечити ефективний аналіз, перевірку й оцінку цифрових доказів, забезпечити правовий захист особи у цифровому просторі, адаптувати кримінальний процес до сучасних умов цифрового інформаційного суспільства.

Висновки. Електронні докази є невід'ємною частиною сучасного кримінального процесу, що зумовлює необхідність їх правового визнання, чіткої регламентації та забезпечення належного рівня захисту. В умовах цифрової трансформації правосуддя належне опрацювання проблематики електронних доказів є запорукою забезпечення принципів змагальності, об'єктивності та справедливості кримінального судочинства в Україні.

Дослідження правового статусу електронних доказів виявляє нагальну потребу оновлення і систематизації чинного законодавства, яке наразі не охоплює усіх аспектів їх використання. Наведене визначає потребу подальших наукових розвідок та окреслює їх напрями. Зокрема, відсутність чітко визначених критеріїв допустимості, стандартів перевірки та оцінки цифрових доказів створює прогалини у правовому регулюванні, що ускладнює і правозастосування. На практиці виникають значні труднощі під час збору таких доказів, що часто зумовлене перешкодами технічного характеру, проблемами з доступом до інформації, розмі-

щеної на хмарних сховищах або серверах за межами національної юрисдикції. Аналіз судової практики свідчить про різноманітність підходів до тлумачення електронних доказів, що

пояснюється відсутністю уніфікованих підходів до розуміння їхньої правової природи, критеріїв оцінки достовірності та допустимості використання у кримінальному провадженні.

Література

1. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (дата звернення: 30.05.2025).
2. Колодіна А.С., Федорова Т.С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права*. 2022. Вип. 1. С. 176–180.
3. 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 : Закон України від 15 березня 2022 року № 2137-IX. URL: <https://zakon.rada.gov.ua/laws/show/2137-20#Text> (дата звернення: 30.05.2025).
4. Скрипник А.В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні : дис. докт. філософ. : 12.00.09. Харків, 2021. 204 с.
5. Вітківська І. Автентичність електронних доказів: практичний аспект. *Право і держава*. 2020. № 48 (1). С. 23–27.
6. Сидоренко М. Використання цифрових доказів у кримінальних справах: правові та технічні аспекти. *Юридичний вісник*. 2021. № 15 (3). С. 14–19.
7. Постанова Верховного Суду від 13 липня 2020. Справа № 753/10840/19. Провадження № 61-22727св19. URL: <https://reyestr.court.gov.ua/Review/90385050> (дата звернення: 02.06.2025).
8. Постанова Верховного Суду від 10 вересня 2020 р. Справа № 751/6069/19. Провадження № 51-1704км20. URL: <https://reyestr.court.gov.ua/Review/91722819> (дата звернення: 04.06.2025).
9. Бондаренко Р. Проблеми процесуального оформлення електронних доказів. *Кримінальний процес*. 2020. № 11 (1). С. 45–50.
10. Ратнова А. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. докт. філософ. : 12.00.09. Львів, 2021. 248 с.
11. Fredesvinda I. The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime – Results of a European Study. *Journal of Digital Forensic Practice*. 2007. No. 1 (4). P. 285–289.
12. Чернявський С.С., Орлов Ю.Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Вісник кримінального судочинства*. 2017. Вип. № 2. С. 112–124.
13. Степанюк Р.Л., Перлін С.І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник Луганського державного університету внутрішніх справ*. 2022. № 3(99). С. 283–294.
14. Цехан Д.М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Серія : «Юриспруденція»*. № 5. 2013. С. 256–260.

References

1. Kryminalnyi protsesualnyi kodeks Ukrainy (2012) [Criminal Procedure Code of Ukraine from April 13 2012]. Retrieved from: <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (data zvernennia: 30.05.2025) [in Ukrainian].
2. Kolodina, A.S., & Fedorova, T.S. (2022) Tsyfrova kryminalistyka: problemy teorii i praktyky [Digital forensics: problems of theory and practice]. *Kyivskiy chasopys prava – Kyiv Journal of Law*, issue 1, 176–180 [in Ukrainian].
3. Zakon Ukrainy pro vnesennia zmin do Kryminalnoho protsesualnoho kodeksu Ukrainy ta Zakonu Ukrainy “Pro elektronni komunikatsii” shchodo pidvyshchennia efektyvnosti dosudovoho rozsliduvannia “za hariachymy slidamy” ta protydii kiberatakham [Law of Ukraine on Amendments to the Criminal Procedural Code and the Law on Electronic Communications to Increase the Efficiency of Pre-trial Investigation “Hot on the Trail” and to Combat Cyberattacks]. (2022, March 15). Retrieved from: <https://zakon.rada.gov.ua/laws/show/2137-20#Text> [in Ukrainian].
4. Skrypnyk, A.V. (2021). Vykorystannia informatsii z elektronnykh nosiiv u kryminalnomu protsesualnomu dokazuvanni [Use of information from electronic media in criminal procedural evidence]. *Doctor’s thesis*. Kharkiv [in Ukrainian].
5. Vitkovska, I. (2020). Avtentychnist elektronnykh dokaziv: praktychnyi aspekt [Authenticity of electronic evidence: a practical aspect]. *Pravo i derzhava – Law and State*, 48(1), 23–27 [in Ukrainian].

6. Sydorenko, M. (2021). Vykorystannia tsyfrovyykh dokaziv u kryminalnykh spravakh: pravovi ta tekhnichni aspekty [Use of digital evidence in criminal cases: legal and technical aspects]. *Yurydychnyi visnyk – Legal Bulletin*, 15(3), 14–19 [in Ukrainian].
7. Verkhovnyi Sud. (2020, July 13). *Postanova u spravi № 753/10840/19, provadzhennia № 61-22727sv19* [Ruling in case No. 753/10840/19, proceeding No. 61-22727sv19]. Retrieved from: <https://reyestr.court.gov.ua/Review/90385050> [in Ukrainian].
8. Verkhovnyi Sud. (2020, September 10). *Postanova u spravi № 751/6069/19, provadzhennia № 51-1704km20* [Ruling in case No. 751/6069/19, proceeding No. 51-1704km20]. Retrieved from: <https://reyestr.court.gov.ua/Review/91722819> [in Ukrainian].
9. Bondarenko, R. (2020). Problemy protsesualnoho oformlennia elektronnykh dokaziv [Problems of procedural formalization of electronic evidence]. *Kryminalnyi protses – Criminal Process*, 11(1), 45–50 [in Ukrainian].
10. Ratnova, A. (2021). *Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv u dokazuvanni* [Criminal procedural and forensic foundations for the use of electronic documents in evidence]. Doctor's thesis. Lviv [in Ukrainian].
11. Fredesvinda, I. (2007). The admissibility of electronic evidence in court (A.E.E.C.): Fighting against high-tech crime – Results of a European study. *Journal of Digital Forensic Practice*, 1(4), 285–289 [in English].
12. Cherniavskiy, S.S., & Orlov, Yu.Yu. (2017). Elektronne vidobrazhennia yak dzherelo dokaziv u kryminalnomu provadzhenni [Electronic representation as a source of evidence in criminal proceedings]. *Visnyk kryminalnoho sudochynstva – Bulletin of Criminal Proceedings*, 2, 112–124 [in Ukrainian].
13. Stepaniuk, R.L., Perlin, S.I. (2022). Tsyfrova kryminalistyka y udoskonalennia systemy kryminalistychnoi tekhniky v Ukraini [Digital forensics and improvement of the forensic technology system in Ukraine]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav – Bulletin of Luhansk State University of Internal Affairs named after E. Didorenko*, 3 (99), 283–294 [in Ukrainian].
14. Tsekhan, D.M. (2013). Tsyfrovi dokazy: poniattia, osoblyvosti ta mistse u systemi dokazuvannia [Digital evidence: concept, features, and place in the system of proof]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Serii: Yurysprudentsiia – Scientific Bulletin of the International Humanitarian University. Series: Law*, 5, 256–260 [in Ukrainian].