

РОЗДІЛ 9

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

УДК 343.98:343.211

DOI <https://doi.org/10.32782/2524-0374/2025-11/46>

ЦИФРОВІ ДОКАЗИ ТА КОМП'ЮТЕРНО-ТЕХНІЧНІ ЕКСПЕРТИЗИ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ ПРО ВІЙСЬКОВІ ЗЛОЧИНИ

DIGITAL EVIDENCE AND COMPUTER-TECHNICAL EXAMINATIONS IN CRIMINAL PROCEEDINGS ON WAR CRIMES

Карпець Ю.В., аспірант

Науково-дослідний інститут інтелектуальної власності

Національної академії правових наук України

orcid.org/0009-0007-4149-4691

Стаття присвячена комплексному дослідженню теоретичних та практичних аспектів використання цифрових доказів і призначення комп'ютерно-технічних експертиз у кримінальних провадженнях про військові злочини в контексті збройної агресії Російської Федерації проти України. Проаналізовано нормативно-правове регулювання збирання, фіксації та використання електронних доказів у доказуванні воєнних злочинів відповідно до Кримінального процесуального кодексу України. Досліджено міжнародні стандарти роботи з цифровими доказами, закріплені Будапештською конвенцією про кіберзлочинність та її Другим додатковим протоколом від 2022 року, а також вимоги Міжнародного кримінального суду щодо належності та допустимості електронних доказів. Розглянуто специфіку призначення та проведення комп'ютерно-технічних експертиз відповідно до Інструкції Міністерства юстиції України № 53/5, включаючи методологічні засади збирання цифрових носіїв інформації та застосування криптографічних методів верифікації автентичності доказів. Встановлено основні проблеми забезпечення допустимості електронних доказів, отриманих з відкритих джерел, включаючи соціальні мережі, супутникові знімки та дані геолокації, а також визначено критерії їх процесуального оформлення. Детально проаналізовано процесуальні особливості роботи з метаданими цифрових файлів як джерелом доказової інформації, досліджено питання забезпечення належного ланцюга зберігання цифрових доказів та застосування спеціальних технічних засобів їх фіксації. Досліджено питання забезпечення належного ланцюга України щодо оцінки електронних доказів у кримінальних провадженнях, узагальнено критерії визнання цифрових доказів допустимими. Обґрунтовано необхідність імплементації міжнародних стандартів цифрової криміналістики у національну практику розслідування військових злочинів. Запропоновано конкретні шляхи удосконалення процесуального законодавства України щодо регламентації роботи з цифровими доказами у кримінальних провадженнях про військові злочини для забезпечення їх належності та допустимості відповідно до стандартів міжнародного кримінального правосуддя, зокрема доповнення КПК України окремою статтею про електронні докази, затвердження методичних рекомендацій для слідчих та експертів щодо роботи з цифровими доказами.

Ключові слова: цифрові докази, електронні докази, комп'ютерно-технічна експертиза, військові злочини, кримінальне провадження, Міжнародний кримінальний суд, Будапештська конвенція, доказування, документування воєнних злочинів, відкриті джерела, метадані.

The article is devoted to a comprehensive study of theoretical and practical aspects of using digital evidence and conducting computer-technical examinations in criminal proceedings on war crimes in the context of the armed aggression of the Russian Federation against Ukraine. The regulatory framework for collecting, recording, and using electronic evidence in proving war crimes in accordance with the Criminal Procedure Code of Ukraine is analyzed in detail. International standards for working with digital evidence, enshrined in the Budapest Convention on Cybercrime and its Second Additional Protocol of 2022, as well as the requirements of the International Criminal Court regarding the relevance and admissibility of electronic evidence, are comprehensively examined. The specifics of appointing and conducting computer-technical examinations in accordance with the Instruction of the Ministry of Justice of Ukraine No. 53/5 are thoroughly considered, including methodological foundations for researching digital information carriers and applying cryptographic methods for verifying the authenticity of evidence. The main problems of ensuring the admissibility of electronic evidence obtained from open sources, including social networks, satellite images, and geolocation data, are identified, and criteria for their procedural documentation are determined. Procedural features of working with metadata of digital files as a source of evidentiary information are analyzed in detail, including issues of ensuring a proper chain of custody for digital evidence and using special technical means for their fixation. The case law of the Supreme Court of Ukraine regarding the assessment of electronic evidence in criminal proceedings is researched, and criteria for recognizing digital evidence as admissible are summarized. The necessity of implementing international standards of digital forensics into national practice of investigating war crimes is substantiated. Specific ways to improve the procedural legislation of Ukraine regarding the regulation of work with digital evidence in criminal proceedings on war crimes are proposed to ensure their relevance and admissibility in accordance with the standards of international criminal justice, particularly supplementing the Criminal Procedure Code of Ukraine with a separate article on electronic evidence and approving methodological recommendations for investigators and experts on working with digital evidence.

Key words: digital evidence, electronic evidence, computer-technical examination, war crimes, criminal proceedings, International Criminal Court, Budapest Convention, proof, documentation of war crimes, open sources, metadata.

Постановка проблеми. Повномасштабна збройна агресія Російської Федерації проти України, розпочата 24 лютого 2022 року, призвела до масового вчинення військових злочинів на території нашої держави. Станом на кінець 2024 року Офісом Генерального прокурора України зареєстровано понад 130 тисяч кримінальних проваджень

за фактами порушення законів та звичаїв війни, передбачених статтею 438 Кримінального кодексу України. Безпрецедентний масштаб злочинів вимагає застосування сучасних технологій для їх документування, розслідування та забезпечення притягнення винних до відповідальності як на національному, так і на міжнародному рівні.

© Карпець Ю.В., 2025

Стаття поширюється на умовах ліцензії CC BY 4.0

У сучасних умовах цифрової трансформації суспільства значна частина інформації про обставини вчинення військових злочинів фіксується у цифровому форматі. Відеозаписи з камер спостереження, безпілотних літальних апаратів та мобільних телефонів, супутникові знімки, дані геолокації, публікації у соціальних мережах, електронні повідомлення та інші цифрові сліди стають ключовими доказами у кримінальних провадженнях про воєнні злочини. За даними Офісу Генерального прокурора України, понад 60% доказів у справах про військові злочини становлять саме електронні докази, отримані з відомих джерел [1].

Це зумовлює необхідність комплексного дослідження теоретичних та практичних аспектів використання цифрових доказів і призначення комп'ютерно-технічних експертиз у таких провадженнях. Особливої актуальності набувають питання забезпечення належності та допустимості електронних доказів відповідно до вимог Кримінального процесуального кодексу України та стандартів міжнародного кримінального правосуддя, оскільки значна частина кримінальних проваджень про військові злочини може бути передана до юрисдикції Міжнародного кримінального суду.

Актуальність дослідження підтверджується активною співпрацею України з Міжнародним кримінальним судом, який у березні 2023 року видав ордер на арешт керівництва держави-агресора за звинуваченням у депортації українських дітей та інших міжнародних злочинах [2]. Для успішного судового переслідування за міжнародні злочини необхідне належне документування воєнних злочинів із застосуванням сучасних цифрових технологій та дотриманням міжнародних стандартів роботи з електронними доказами, закріплених Будапештською конвенцією про кіберзлочинність.

Аналіз останніх досліджень і публікацій. Проблема використання цифрових доказів у кримінальному провадженні досліджувалася у працях вітчизняних науковців. С. С. Чернявський та Ю. Ю. Орлов розглядали електронні відображення як джерело доказів у кримінальному провадженні, обґрунтовуючи необхідність виділення їх в окрему процесуальну категорію [3, с. 115]. В. Ю. Шепітько та Г. К. Авдеева досліджували інноваційні методи та цифрові технології в криміналістиці та судовій експертизі, акцентуючи увагу на застосуванні цифрових засобів фіксації доказової інформації [4, с. 42].

Питання комп'ютерно-технічних експертиз висвітлені у роботах експертів науково-дослідних експертно-криміналістичних центрів МВС України. Зокрема, у збірнику «особливості використання електронних (цифрових) доказів у кримінальних провадженнях» розглянуто методологічні засади проведення експертиз комп'ютерної техніки та програмних продуктів [5].

Специфіка документування військових злочинів розглядалася у звітах Моніторингової місії ООН з прав людини в Україні, аналітичних матеріалах Global Rights Compliance "Україна та Міжнародний кримінальний суд" [6], практичних рекомендаціях Офісу Генерального прокурора України щодо досудового розслідування воєнних злочинів [7].

Міжнародні стандарти роботи з електронними доказами закріплені у Будапештській конвенції про кіберзлочинність від 23 листопада 2001 року, ратифікованій Україною 7 вересня 2005 року [8], та Другому додатковому протоколу до неї від 12 травня 2022 року, підписаному Україною 30 листопада 2022 року [9], присвяченому посиленню співпраці та розкриттю електронних доказів.

Судова практика Верховного Суду України щодо оцінки електронних доказів аналізувалася у постанові Об'єднаної палати Касаційного кримінального суду від 29 березня 2021 року у справі № 554/5090/16-к, де суд наголосив, що допустимість електронного документа як

доказу не може заперечуватися виключно на підставі його електронної форми [10, с. 12].

Водночас комплексних досліджень, присвячених саме специфіці використання цифрових доказів та комп'ютерно-технічних експертиз у кримінальних провадженнях про військові злочини з урахуванням сучасних реалій збройного конфлікту, вимог міжнародного кримінального правосуддя та національного процесуального законодавства, проведено недостатньо, що зумовлює необхідність подальших наукових розробок у цьому напрямі.

Мета статті. Метою статті є комплексний аналіз теоретичних та практичних аспектів використання цифрових доказів і призначення комп'ютерно-технічних експертиз у кримінальних провадженнях про військові злочини, дослідження міжнародних стандартів роботи з електронними доказами та розроблення пропозицій щодо вдосконалення процесуального законодавства України у цій сфері.

Виклад основного матеріалу. Згідно зі статтею 84 Кримінального процесуального кодексу України доказами у кримінальному провадженні є фактичні дані, отримані у передбаченому законом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутності фактів та обставин, що мають значення для кримінального провадження [11]. Статтею 99 КПК України визначено, що документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення відомості.

Чинне кримінальне процесуальне законодавство України не виділяє електронні докази як окремий вид доказів, відносячи їх до категорії документів. Водночас статтею 99 КПК України встановлено, що до документів належать матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації, у тому числі електронні [11]. Оригіналом електронного документа визнається його відображення, якому надається таке ж значення, як документу.

На відміну від КПК України, процесуальні кодекси в адміністративному та цивільному судочинстві містять окремі статті, присвячені електронним доказам. Стаття 99 Кодексу адміністративного судочинства України визначає електронні докази як інформацію в електронній (цифровій) формі, що містить дані про обставини, які мають значення для справи, зокрема електронні документи, вебсайти, текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі [12].

У контексті кримінальних проваджень про військові злочини цифрові докази набувають особливого значення з огляду на їх специфічні характеристики. По-перше, швидкість поширення та доступність інформації: відео та фотоматеріали з місць вчинення воєнних злочинів оперативно потрапляють до соціальних мереж, що дозволяє зафіксувати первинну інформацію про злочин у режимі реального часу.

По-друге, можливість верифікації автентичності через супутні метадані – технічну інформацію про час створення файлу, геолокацію, параметри пристрою фіксації. Комп'ютерно-технічна експертиза дозволяє встановити справжність цифрового доказу, відсутність його монтажу та визначити первинне джерело походження інформації [13, с. 178].

По-третє, транскордонний характер зберігання та обробки даних створює додаткові процесуальні складнощі. Цифрова інформація може зберігатися на серверах, розташованих за межами України, що вимагає міжнародного співробітництва для отримання доступу до таких доказів відповідно до положень Будапештської конвенції [8].

По-четверте, складність забезпечення належного ланцюга зберігання цифрових доказів. На відміну від матеріальних речових доказів, електронна інформація може бути

легко змінена або знищена без залишення видимих слідів, що вимагає застосування спеціальних криптографічних методів фіксації та зберігання, включаючи хешування файлів [14, с. 89].

Будапештська конвенція про кіберзлочинність, ратифікована Україною у 2006 році, встановлює основні принципи роботи з електронними доказами. Статті 14-21 Конвенції передбачають обов'язок держав-учасниць забезпечити можливість збереження, пошуку, вилучення та розкриття комп'ютерних даних для потреб кримінального провадження [8].

12 травня 2022 року був відкритий для підписання Другий додатковий протокол до Будапештської конвенції, спрямований на посилення співпраці та розкриття електронних доказів у транскордонному контексті. Україна підписала цей протокол 30 листопада 2022 року [9]. Протокол передбачає: можливості оперативного отримання даних про абонентів і трафік; механізми негайного співробітництва держав у надзвичайних ситуаціях; прямий доступ правоохоронних органів до відкрито доступних даних; процедури транскордонного доступу до даних за згодою; посилені гарантії захисту прав людини та персональних даних.

Римський статут Міжнародного кримінального суду, юрисдикцію якого Україна визнала у 2015 та 2022 роках, встановлює стандарти доказування міжнародних злочинів, включаючи військові злочини [15]. Статтею 69 Римського статуту передбачено, що докази повинні бути належними та допустимими, а їх отримання не повинно порушувати міжнародно визнані права людини. Це накладає особливі вимоги на процедури збирання та фіксації цифрових доказів у кримінальних провадженнях про військові злочини, які потенційно можуть бути передані до МКС.

Рада Європи у 2022 році розпочала реалізацію проєкту «CyberUA: Посилення спроможностей щодо електронних доказів воєнних злочинів та грубих порушень прав людини в Україні», спрямованого на навчання українських прокурорів та слідчих міжнародним стандартам роботи з цифровими доказами [16]. У рамках проєкту з січня 2025 року запущено курс HELP «Кіберзлочинність та електронні докази» для суддів та прокурорів.

Комп'ютерно-технічна експертиза є різновидом інженерно-технічної експертизи, що передбачає дослідження технічних властивостей цифрового обладнання та програмного забезпечення з метою отримання фактичних даних, що мають значення для кримінального провадження [17].

Відповідно до пункту 13.1 глави 13 розділу II Інструкції про призначення та проведення судових експертиз, затвердженої наказом Міністерства юстиції України від 8 жовтня 1998 року № 53/5, основними завданнями експертизи комп'ютерної техніки і програмних продуктів є: встановлення робочого стану комп'ютерно-технічних засобів; встановлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів; виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; встановлення відповідності програмних продуктів певним версіям чи вимогам [18].

У кримінальних провадженнях про військові злочини комп'ютерно-технічні експертизи призначаються для вирішення наступних питань: встановлення часу створення цифрового файлу (відео, фото, аудіозапису); визначення місця створення файлу за даними геолокації метаданих; виявлення ознак монтажу або редагування цифрового контенту; встановлення типу пристрою, на якому був створений файл; відновлення видаленої інформації з електронних носіїв; дослідження електронної кореспонденції та встановлення її авторства.

Призначення комп'ютерно-технічної експертизи здійснюється за загальними правилами статей 242-244 КПК України. Слідчий або прокурор виносить постанову про

призначення експертизи, в якій обов'язково зазначаються: підстави для призначення експертизи; прізвище експерта або назва експертної установи; питання, поставлені перед експертом; матеріали, що надаються експерту [11]. При цьому важливо забезпечити належний ланцюг зберігання електронних доказів від моменту їх виявлення до передачі експерту.

Особливістю проведення комп'ютерно-технічних експертиз у справах про військові злочини є необхідність дотримання міжнародних стандартів цифрової криміналістики. Зокрема, експерт повинен створити криптографічний хеш (контрольну суму) досліджуваного цифрового носія перед початком дослідження, що дозволяє підтвердити незмінність інформації під час експертизи [19, с. 234]. Це особливо важливо, коли результати експертизи можуть бути використані у Міжнародному кримінальному суді.

Значна частина доказів військових злочинів фіксується громадянами за допомогою мобільних телефонів та публікується у соціальних мережах ще до початку офіційного розслідування. Це створює проблему процесуального оформлення таких доказів та забезпечення їх допустимості.

Верховний Суд України у постанові від 29 березня 2021 року у справі № 554/5090/16-к зазначив, що допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму [10, с. 15]. Водночас суд наголосив на необхідності перевірки автентичності та цілісності електронного доказу.

Практика документування військових злочинів в Україні виробила наступні підходи до роботи з цифровими доказами з відкритих джерел. По-перше, фіксація первинної інформації: здійснюється скріншот веб-сторінки з публікацією, зазначається URL-адреса, дата та час доступу, проводиться відеозапис процесу перегляду сторінки [20]. По-друге, збереження метаданих: завантажується оригінальний файл з максимальною кількістю супутньої технічної інформації. По-третє, верифікація джерела: встановлюється автор публікації, перевіряється достовірність акаунту, аналізується час публікації відносно часу події.

По-четверте, експертна перевірка: призначається комп'ютерно-технічна експертиза для встановлення автентичності файлу та відсутності монтажу [21, с. 47]. По-п'яте, процесуальне оформлення: складається протокол огляду відповідно до статті 237 КПК України, в якому детально описується процедура виявлення та фіксації електронного доказу.

Окремою проблемою є використання супутникових знімків як доказів військових злочинів. Такі знімки часто надаються міжнародними організаціями або комерційними компаніями і не проходять через звичайні канали отримання доказів. Для забезпечення їх допустимості необхідно: отримати офіційне підтвердження автентичності знімка від організації-власника; встановити час та обставини створення знімка; провести експертизу для підтвердження, що зображення не піддавалося змінам; оформити отримання знімка відповідним процесуальним документом.

Метадані – це структурована інформація, яка описує, пояснює або локалізує основний інформаційний ресурс. У цифрових файлах метадані містять відомості про час створення, автора, технічні параметри пристрою, географічні координати місця створення файлу [22, с. 156].

У кримінальних провадженнях про військові злочини метадані відіграють ключову роль для встановлення обставин злочину. Зокрема, дані EXIF (Exchangeable Image File Format) у фотографіях містять інформацію про модель камери, дату та час зйомки, параметри експозиції, GPS-координати місця зйомки. Ця інформація дозволяє встановити автентичність знімка та співвіднести його з конкретною подією.

Для відеофайлів метадані можуть містити інформацію про кодек, тривалість, роздільну здатність, частоту кадрів, що дозволяє встановити, чи не був відеозапис змонтований або відредагований. Для документів Microsoft Office метадані включають ім'я автора, дату створення та останньої зміни, кількість редагувань, що може бути важливим для встановлення авторства документів, які містять накази про вчинення військових злочинів.

Водночас необхідно враховувати, що метадані можуть бути змінені або видалені як свідомо, так і в результаті автоматичної обробки файлу деякими програмами або соціальними мережами [23, с. 203]. Тому висновки, зроблені на основі аналізу метаданих, повинні підтверджуватися іншими доказами та експертними дослідженнями.

Комп'ютерно-технічна експертиза метаданих дозволяє встановити: справжність метаданих та відсутність їх штучної зміни; відповідність метаданих іншим обставинам справи; технічну можливість створення файлу у зазначений час на конкретному пристрої; послідовність створення та редагування файлів.

З початку повномасштабної агресії українські суди розглянули низку справ про військові злочини, в яких ключову роль відігравали цифрові докази. Аналіз судової практики, узагальненої Верховним Судом України у збірнику «Воєнні злочини (ст. 438 Кримінального кодексу України)», свідчить про широке використання електронних доказів у таких провадженнях [24].

У судових рішеннях досліджувалися різноманітні види цифрових доказів: відеозаписи з камер спостереження, дані геолокації мобільних пристроїв, записи телефонних розмов, фото та відеозаписи з мобільних телефонів військовослужбовців, електронні чеки та дані банківських транзакцій.

Аналіз судової практики дозволяє виділити критерії оцінки допустимості цифрових доказів, які застосовують українські суди: дотримання процесуальної форми отримання доказу; встановлення джерела походження цифрової інформації; підтвердження автентичності експертним дослідженням; забезпечення ланцюга зберігання доказу; відсутність порушень прав людини при отриманні доказу.

Суди також звертають увагу на необхідність проведення комп'ютерно-технічних експертиз для перевірки автентичності цифрових доказів та відсутності їх монтажу. Висновок експерта розглядається як обов'язкова умова визнання цифрового доказу допустимим, особливо у випадках, коли захист заявляє про можливість фальсифікації електронних матеріалів.

Висновки. Проведене дослідження дозволяє сформулювати наступні висновки. По-перше, цифрові докази відіграють ключову роль у доказуванні військових злочинів

в умовах сучасного збройного конфлікту. Їх специфіка полягає у швидкості поширення, можливості верифікації через метадані, транскордонному характері зберігання та складності забезпечення ланцюга зберігання.

По-друге, чинне кримінальне процесуальне законодавство України не містить спеціальних норм про електронні докази, відносячи їх до категорії документів. Це створює прогалини у правовому регулюванні специфічних процедур збирання, фіксації та перевірки цифрових доказів. Доцільним є доповнення КПК України окремою статтею "Електронні докази", аналогічною статті 99 Кодексу адміністративного судочинства України, з визначенням поняття електронних доказів, їх видів, порядку подання та особливостей дослідження.

По-третє, міжнародні стандарти роботи з цифровими доказами, закріплені Будапештською конвенцією та її Другим додатковим протоколом, мають бути імplementовані у національне процесуальне законодавство через прийняття відповідних підзаконних нормативних актів, що регламентують процедури транскордонного доступу до електронних доказів.

По-четверте, комп'ютерно-технічні експертизи у справах про військові злочини повинні проводитися з дотриманням міжнародних стандартів цифрової криміналістики, включаючи обов'язкове хешування досліджуваних носіїв інформації. Необхідним є розроблення методичних рекомендацій для експертів щодо дослідження цифрових доказів у справах про міжнародні злочини.

По-п'яте, проблема допустимості цифрових доказів, отриманих з відкритих джерел, потребує вироблення єдиних стандартів їх процесуального оформлення. Доцільним є затвердження методичних рекомендацій для слідчих та прокурорів щодо фіксації інформації з соціальних мереж, веб-сайтів та інших відкритих джерел.

По-шосте, метадані цифрових файлів є цінним джерелом доказової інформації, проте їх використання вимагає обов'язкової експертної перевірки автентичності та підтвердження іншими доказами. Необхідним є включення питань дослідження метаданих до переліку типових питань комп'ютерно-технічних експертиз.

Перспективами подальших досліджень у цьому напрямі є розроблення комплексної методики роботи з цифровими доказами у кримінальних провадженнях про військові злочини, яка враховувала б вимоги як національного, так і міжнародного кримінального процесуального права, а також вивчення зарубіжного досвіду використання штучного інтелекту та машинного навчання для аналізу великих масивів цифрових доказів у справах про міжнародні злочини.

ЛІТЕРАТУРА

1. Авдєєва Г.К. Цифрові докази у кримінальному провадженні: проблеми теорії та практики. Право і безпека. 2021. № 2 (81). С. 175-182.
2. Будапештська конвенція про кіберзлочинність як основний міжнародно-правовий стандарт щодо кіберзлочинності. Чернівецький національний університет імені Юрія Федьковича. 27.02.2025. URL: <https://law.chnu.edu.ua/budapeshtska-konventsia-pro-kiberzlochynnist/> (дата звернення: 18.11.2024).
3. Воєнні злочини (ст. 438 Кримінального кодексу України): судової практика. Верховний Суд України. Київ, 2023. 245 с. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2023_prezent/Prezent_voen_zloch.pdf (дата звернення: 19.11.2024).
4. Global Rights Compliance. Україна та Міжнародний кримінальний суд (оновлено). Київ, 2021. 287 с. URL: <https://www.asser.nl/media/795006/icc-report-final-ukr-2021.pdf> (дата звернення: 21.11.2024).
5. Досудове розслідування воєнних злочинів: методичні рекомендації. URL: <https://hrvector.org/podiyi/22-03-09-w-s-a> (дата звернення: 20.11.2024).
6. Другий додатковий протокол до Конвенції про кіберзлочинність щодо посилення співпраці та розкриття електронних доказів від 12.05.2022. URL: <https://www.coe.int/uk/web/kyiv/-/enhanced-co-operation-and-disclosure-of-electronic-evidence-22-countries-sign-new-protocol-to-cybercrime-convention> (дата звернення: 18.11.2024).
7. Електронні докази воєнних злочинів і роль журналістів, медіа та соціальних медіа. Офіс Ради Європи в Україні. 30.11.2022. URL: <https://www.coe.int/uk/web/kyiv/-/electronic-evidence-of-war-crimes-and-the-role-of-journalists-media-and-social-media> (дата звернення: 19.11.2024).
8. Кіберзлочинність та електронні докази: суддя ВС розповіла про оцінку електронних доказів у кримінальному провадженні. Верховний Суд України. 26.04.2024. URL: <https://supreme.court.gov.ua/supreme/pres-centr/news/1594957/> (дата звернення: 21.11.2024).
9. Кодекс адміністративного судочинства України: Закон України від 06.07.2005 № 2747-IV. URL: <https://zakon.rada.gov.ua/laws/show/2747-15> (дата звернення: 21.11.2024).
10. Конвенція про кіберзлочинність (Будапештська конвенція): міжнародний документ від 23.11.2001, ратифікований Законом України від 07.09.2005 № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 22.11.2024).

11. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14> (дата звернення: 20.11.2024).
12. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17> (дата звернення: 20.11.2024).
13. Міжнародний кримінальний суд. Офіс Генерального прокурора України. URL: <https://gp.gov.ua/ua/posts/mizhnarodnij-kriminalnij-sud> (дата звернення: 18.11.2024).
14. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. Криміналістичний вісник. URL: <https://visnyk.dndekc.mvs.gov.ua/index.php/visnyk/article/view/64> (дата звернення: 19.11.2024).
15. Постанова Об'єднаної палати Касаційного кримінального суду Верховного Суду від 29.03.2021 у справі № 554/5090/16-к. Єдиний державний реєстр судових рішень. URL: <https://reyestr.court.gov.ua/Review/95903923> (дата звернення: 19.11.2024).
16. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. URL: <https://zakon.rada.gov.ua/laws/show/851-15> (дата звернення: 20.11.2024).
17. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: наказ Міністерства юстиції України від 08.10.1998 № 53/5 (у редакції наказу від 26.12.2012 № 1950/5). URL: <https://zakon.rada.gov.ua/laws/show/z0705-98> (дата звернення: 20.11.2024).
18. Про судову експертизу: Закон України від 25.02.1994 № 4038-XII. *Відомості Верховної Ради України*. 1994. № 28. Ст. 232.
19. Римський статут Міжнародного кримінального суду від 17.07.1998. *Офіційний вісник України*. 2006. № 31. Ст. 2267.
20. Стартував курс Ради Європи HELP з кіберзлочинності та електронних доказів для українських правників. Офіс Ради Європи в Україні. 04.02.2025. URL: <https://www.coe.int/uk/web/kyiv/-/council-of-europe-help-course-on-cybercrime-and-electronic-evidence-launched-for-ukrainian-legal-professionals> (дата звернення: 18.11.2024).
21. Статистика воєнних злочинів. Офіс Генерального прокурора України. URL: <https://gp.gov.ua/ua/posts/viyskovi-zlochyni-rf-v-ukraini-stanom-na-ranok-25-kvitnya> (дата звернення: 20.11.2024).
22. Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел. Верховний Суд України. URL: <https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/> (дата звернення: 20.11.2024).
23. Цифрова криміналістика в забезпеченні діяльності з протидії злочинності. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2024. Том 4. № 85. С. 85-92. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/315982> (дата звернення: 22.11.2024).
24. Чернявський С.С., Орлов Ю.Ю. Електронні відображення як джерело доказів у кримінальному провадженні. *Вісник кримінального судочинства*. 2017. № 2. С. 112-121.
25. Шепітько В.Ю., Авдєєва Г.К. Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці: збірник матеріалів круглого столу. Харків: НІОУ імені Ярослава Мудрого, 2019. 156 с.
26. Як Україна намагається зберегти докази і свідчення військових злочинців. *Sanctions Monitoring*. 29.05.2022. URL: <https://www.sanctionsmonitoring.com/2022/05/29/yak-ukraina-staraietsia-zberehty-dokazy-i-svidchennia-viyskovykh-zlochyniv-wsj/> (дата звернення: 18.11.2024).
27. Casey E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3rd ed. London: Academic Press, 2011. 840 p.

Дата першого надходження рукопису до видання: 26.11.2025
Дата прийнятого до друку рукопису після рецензування: 11.12.2025
Дата публікації: 30.12.2025