МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова праця
на правах рукопису

ГАЛЬЧЕНКО ВІКТОРІЯ СЕРГІЇВНА

УДК 343.13; 343.98:004

ДИСЕРТАЦІЯ
НАЛЕЖНІСТЬ І ДОПУСТИМІСТЬ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

08 – Право
081 – Право

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ **В. С. Гальченко**

Науковий керівник: **Дубівка Ірина Володимирівна**,
кандидат юридичних наук, доцент

Київ–2026

АНОТАЦІЯ

Гальченко В. С. Належність і допустимість електронних доказів у кримінальному провадженні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 «Право». – Національна академія внутрішніх справ, Київ, 2026.

Дисертацію присвячено дослідженню належності й допустимості електронних доказів у кримінальному провадженні. Доведено, що електронні докази є самостійним і специфічним феноменом доказування, який не зводиться ні до традиційних письмових, ні до речових доказів. Вони уособлюють особливу природу інформації, що існує в множинних і рівноцінних екземплярах, формує власні ризики для автентичності, цілісності й відтворюваності процесуальних дій, тому потребує чітко визначених процедур виявлення, фіксації, копіювання, зберігання та перевірки.

Виокремлено кілька наукових підходів до тлумачення сутності електронних доказів: 1) інформаційний, відповідно до якого більшість учених вважає, що електронні докази – це дані (інформація), що виникли внаслідок використання комп'ютерної техніки й можуть бути використані в судовому процесі; 2) об'єктний, згідно з яким електронні докази розглядають як об'єкти цифрового (електронного) середовища, що можуть містити інформацію, важливу для кримінального провадження. Носієм доказової інформації є нематеріальний об'єкт – файл, електронний запис, тобто елемент віртуального простору; 3) комплексний (технологічний), який розглядає електронний доказ як такий, що отриманий з даних, які містяться в будь-якому пристрої або генеруються таким пристроєм, функціонування якого залежить від програмного забезпечення чи даних, що зберігають або передають через комп'ютерну систему чи мережу.

Визначено, що оригіналом електронного технічного документа є той, який створений та зберігається на первинному носії інформації, натомість дублікатом (копією) є його копіювання, переміщення, поширення на інші носії даних. Акцентовано, що (а) роздруківка вебсторінки, частини відео, фото чи іншого файлу не можуть бути визнані ні оригіналом, ні копією електронного документа та не мають самостійного доказового значення; (б) візуалізована в паперовій формі сторінка може бути тільки додатком до проведеної слідчої (розшукової) дії. Зауважено, що належне виготовлення дубліката електронного документа забезпечує його допустимість під час перевірки доказів у суді.

Виокремлено та схарактеризовано проблемні питання використання електронних доказів у кримінальному провадженні, серед яких: 1) невідмежованість електронного доказу від інших джерел доказів; 2) невизначеність джерел одержання електронних доказів у кримінальному провадженні; 3) недостатність нормативно-правового регулювання щодо використання копій електронних доказів, оригінали яких утрачено; 4) обмеження процесуальних можливостей дізнавача щодо збирання електронних доказів; 5) неорганізованість роботи інформаційно-телекомунікаційної системи досудового розслідування за участю Національної поліції України.

На підставі дослідження міжнародного досвіду (Австрія, Болгарія, Велика Британія, Італія, Китайська Народна Республіка, Німеччина, Португалія, США, Чехія, Франція, Швеція) з'ясовано, що в більшості країн електронні дані визнають повноцінним видом доказів, рівнозначним традиційним письмовим чи речовим доказам, незалежно від наявності спеціального визначення в національному законодавстві. З'ясовано, що хоча законодавство переважної більшості досліджуваних країн не містить специфічного закону про електронні докази в кримінальному процесі, зарубіжна правозастосовна практика фокусує увагу на важливості дотримання принципу незмінності даних (жодного редагування оригіналу),

документування всіх дій з електронним носієм і використання належних методів цифрової криміналістики, дотримання встановлених процесуальних вимог і технічних стандартів, щоб гарантувати автентичність та цілісність даних тощо.

Встановлено, що відповідно до практики Європейського суду з прав людини збирання та оцінка електронних доказів передбачає дотримання права на повагу до приватного й сімейного життя. Питання порушення такого права слід розглядати з позиції «розумного очікування конфіденційності». Висвітлено основні позиції Європейського суду з прав людини в частині досліджуваного питання, відповідно до яких: 1) у сферу захисту права, передбаченого ст. 8 Конвенції, потрапляють не лише особисті відносини, а й різноманітні аспекти цифрових комунікацій (телефонні дзвінки, електронні листи, повідомлення, відомості про користування інтернетом на робочому місці тощо); 2) будь-яка форма цифрового нагляду повинна мати чітке законодавче підґрунтя та відповідати критеріям передбачуваності (моніторинг цифрових комунікацій без жодного нормативного акта чи внутрішньої політики не відповідає «вимозі передбаченості закону»); 3) втручання має бути необхідним у демократичному суспільстві, мати законну мету («охорона національної безпеки, запобігання злочинам, захист прав жертв») і бути пропорційним обставинам («серйозність злочинів й обмежений характер спостереження»).

З'ясовано, що електронні докази охоплюють широкий спектр інформації – від файлів і листувань у месенджерах до записів камер спостереження й даних із хмарних сховищ. Їх належність у кримінальному провадженні зумовлена зв'язком із предметом доказування, що потребує ретельної ідентифікації користувача, джерела походження та часових меж. Акцентовано на питанні автентичності, зокрема цифровий доказ слід вважати належним лише тоді, коли його можна об'єктивно пов'язати з досліджуваними подією, особою чи обставиною. Визначено «мінімальний стандарт» належності електронних доказів, що передбачає: ідентифікацію цифрових даних (зв'язок

із користувачем/пристроєм/акаунтом), їх локалізацію (місце/сховище/сервіс), прив’язку в часі (timestamp/метадані) і відтворення (можливість отримати перевірену копію).

Обґрунтовано важливість дотримання принципу «ланцюга збереження доказів» (chain of custody), відповідно до якого кожен етап роботи з електронними даними – виявлення, копіювання, зберігання та передача – має бути задокументовано й перевірено. Зазначено, що використання технічних методів підтвердження автентичності (електронні підписи, контрольні хеш-суми, форензичні образи) створює підґрунтя для визнання доказів достовірними й виключає можливість їх непомітної модифікації. Брак зазначеного технічного підтвердження зумовлює ускладнення судової оцінки цифрових доказів.

Запропоновано на законодавчому рівні закріпити визначення електронного (цифрового) доказу як самостійного джерела з відповідними правилами поводження з ним шляхом внесення змін до ст. 84 Кримінального процесуального кодексу України. Засвідчено необхідність розроблення підзаконних нормативних актів або офіційних методичних рекомендацій для слідчих і судів щодо роботи із цифровими доказами, які встановлюватимуть стандарти фіксації та зберігання електронних даних. Аргументовано доцільність підвищення рівня технічної оснащеності та кваліфікації правоохоронних органів у галузі комп’ютерної криміналістики, щоб забезпечити належну реалізацію нових норм на практиці.

На підставі аналізу наукових позицій визначено, що стандарти доказування поєднують: 1) об’єктивний критерій, що полягає в законодавчо визначених вимогах до кількості та якості доказів, 2) суб’єктивний критерій, який відображає рівень внутрішнього переконання слідчого, прокурора чи суду, що формується на підставі всебічного, повного й неупередженого дослідження обставин справи. Така комбінація критеріїв забезпечує баланс між вимогами процесуальної форми та пізнавальною природою доказування.

Позитивно оцінено зміни, внесені до ч. 4 ст. 99 Кримінального процесуального кодексу України, згідно з якими копії інформації (зокрема комп'ютерних даних), отримані слідчим або прокурором із залученням спеціаліста, суд визнає як оригінал документа. Аналізована норма фактично легалізує застосування криміналістичних методів копіювання цифрових даних та означає, що якщо слідчий за участю спеціаліста з інформаційних технологій скопіює потрібні файли з комп'ютера чи іншої електронної системи на окремий носій, копія матиме таку саму доказову силу, як і початковий носій інформації. Тобто законодавець відійшов від імперативної вимоги обов'язкового вилучення технічних засобів (серверів, мобільних пристроїв) і дозволив використання належно завірених копій електронних документів як джерела доказів, забезпечуючи необхідний баланс між ефективністю досудового розслідування та захистом майнових прав володільців техніки. Водночас виокремлено недоліки аналізованого вище законодавчого положення, що полягають у відсутності детальної процедури долучення, реєстрації та зберігання таких електронних доказів у матеріалах кримінального провадження з визначенням кола відповідальних осіб.

Окреслено алгоритм вилучення цифрового носія, що передбачає: 1) вчинення дій, що унеможливлюють зміну даних на ньому після вилучення (наприклад, вимкнення живлення комп'ютера, використання спеціальних блокувальних пристроїв для портів, поміщення смартфона в екранований контейнер для блокування сигналів тощо); 2) фіксацію всіх обставин, пов'язаних із вилученням, а саме: час вилучення, коло осіб, які мали доступ, серійні номери техніки, стан пристрою (ввімкнений чи вимкнений), наявність запаролення або шифрування тощо; 3) невідкладне дублювання даних (створення копії) у присутності понятих або з використанням безперервного відеозапису із залученням ІТ-спеціаліста.

Акцентовано на поступовій трансформації судової практики в питаннях використання електронних доказів у кримінальному провадженні від їх сприйняття як різновиду документів до визнання самостійним джерелом

доказової інформації. Основні зміни в підходах судів до електронних доказів стосуються: 1) упровадження сталих критеріїв оцінки цифрових даних (автентичність, цілісність, належність і допустимість); 2) розширення кола допустимих електронних доказів (від відеозаписів камер спостереження до скриншотів із месенджерів, GPS-координат чи метаданих файлів); 3) оцінки таких матеріалів з огляду на презумпцію їх надійності, якщо не доведено протилежне. Водночас констатовано, що брак визначення дефініції «електронні докази» в положеннях Кримінального процесуального кодексу України призводить до неоднозначності правозастосування зазначеного інституту.

Ключові слова: доказування, джерело доказів, допустимість доказів, достатність доказів, належність доказів, електронний доказ, електронне доказування, кримінальне провадження.

ABSTRACT

Halchenko V. Propriety and admissibility of electronic evidence in criminal proceedings. – Qualification scientific work as a manuscript.

Dissertation for the degree of Doctor of Philosophy in the specialty 081 «Law». – National Academy of Internal Affairs, Kyiv, 2026.

The dissertation is devoted to the study of the propriety and admissibility of electronic evidence in criminal proceedings.

The dissertation is devoted to the study of the relevance and admissibility of electronic evidence in criminal proceedings. It has been established that electronic evidence constitutes an independent and specific phenomenon of proof, which cannot be reduced either to traditional documentary evidence or to physical evidence. Electronic evidence embodies the unique nature of information existing in multiple equivalent copies, creating specific risks related to authenticity, integrity, and reproducibility of procedural actions. Therefore, it requires clearly defined procedures for detection, collection, recording, copying, preservation, and verification.

Several scientific approaches to the interpretation of the essence of electronic evidence have been identified: (1) the informational approach, according to which most scholars consider electronic evidence as data (information) generated through the use of computer technologies and capable of being used in judicial proceedings; (2) the object-oriented approach, under which electronic evidence is regarded as objects of the digital (electronic) environment containing information relevant to criminal proceedings. In this context, evidentiary information is embodied in an intangible object, such as a file or electronic record, representing an element of virtual space; and (3) the comprehensive (technological) approach, according to which electronic evidence is understood as evidence derived from data contained in or generated by any device whose operation depends on software or data stored or transmitted through a computer system or network.

It has been determined that the original electronic technical document is the document created and stored on the primary information carrier, whereas its duplicate (copy) is produced through copying, transferring, or distributing it to other data storage media. It is emphasized that: (a) a printout of a webpage, part of a video recording, photograph, or any other file cannot be recognized either as the original or as a copy of an electronic document and therefore has no independent evidentiary value; (b) a webpage reproduced in paper form may serve only as an attachment to the relevant investigative (search) action. It is noted that the proper creation of a duplicate of an electronic document ensures its admissibility during judicial examination of evidence.

The study identifies and characterizes the key problematic issues concerning the use of electronic evidence in criminal proceedings, including: (1) the lack of distinction between electronic evidence and other sources of evidence; (2) uncertainty regarding the sources from which electronic evidence may be obtained in criminal proceedings; (3) insufficient legal regulation governing the use of copies of electronic evidence when the originals have been lost; (4) limitations on the procedural powers of inquiry officers in collecting electronic evidence; and (5) the inadequate organization of the information and telecommunication system of pre-trial investigation involving the National Police of Ukraine.

Based on the analysis of international experience (Austria, Bulgaria, the United Kingdom, Italy, the People’s Republic of China, Germany, Portugal, the United States, the Czech Republic, France, and Sweden), it has been established that in most countries electronic data are recognized as a full-fledged type of evidence equivalent to traditional documentary or physical evidence, regardless of whether a specific definition exists in national legislation. Although the legislation of the majority of the studied countries does not contain a separate law regulating electronic evidence in criminal proceedings, foreign law-enforcement practice focuses on the importance of maintaining data integrity (prohibiting any alteration of original data), documenting all actions performed with electronic media, applying

appropriate digital forensic methods, and complying with procedural requirements and technical standards to ensure authenticity and integrity of data.

It has been established that, according to the case law of the European Court of Human Rights, the collection and assessment of electronic evidence must comply with the right to respect for private and family life. Issues concerning interference with this right should be assessed through the concept of a "reasonable expectation of privacy." The principal positions of the European Court of Human Rights regarding this issue have been highlighted, according to which: (1) the protection afforded by Article 8 of the Convention extends not only to personal relationships but also to various aspects of digital communications, including telephone calls, emails, messages, and information concerning internet use in the workplace; (2) any form of digital surveillance must have a clear legal basis and satisfy the requirement of foreseeability, meaning that monitoring digital communications without an appropriate legal framework or internal policy fails to meet the "quality of law" requirement; and (3) interference must be necessary in a democratic society, pursue a legitimate aim (such as national security, crime prevention, or protection of victims' rights), and be proportionate to the circumstances, taking into account the seriousness of the offences and the limited scope of surveillance.

It has been established that electronic evidence encompasses a broad range of information, including files, communications in messaging applications, surveillance camera recordings, and cloud storage data. Its relevance in criminal proceedings is determined by its connection to the subject matter of proof, which requires careful identification of the user, source of origin, and temporal framework. Particular emphasis is placed on authenticity, since digital evidence should be regarded as relevant only where it can be objectively linked to the event, person, or circumstance under investigation. A "minimum standard" of relevance of electronic evidence has been formulated, encompassing identification of digital data (linkage to a user, device, or account), localization (storage location, repository, or service), temporal attribution (timestamps and metadata), and reproducibility (the ability to obtain a verified copy).

The importance of adhering to the principle of the chain of custody has been substantiated. According to this principle, every stage of handling electronic data including detection, copying, storage, and transfer must be properly documented and verified. It is noted that the use of technical methods for confirming authenticity (electronic signatures, hash values, and forensic images) provides the basis for recognizing evidence as reliable and prevents undetectable modifications. The absence of such technical verification significantly complicates judicial assessment of digital evidence.

It is proposed to establish at the legislative level a definition of electronic (digital) evidence as an independent source of evidence, together with specific rules governing its handling, through amendments to Article 84 of the Criminal Procedure Code of Ukraine. The necessity of developing subordinate regulations or official methodological guidelines for investigators and courts regarding the handling of digital evidence has been substantiated. Such instruments should establish standards for the collection and preservation of electronic data. Furthermore, it is argued that the technical capabilities and professional qualifications of law-enforcement agencies in the field of digital forensics should be enhanced to ensure effective implementation of the proposed legal provisions.

Based on the analysis of scholarly approaches, it has been established that standards of proof combine: (1) an objective criterion, consisting of legislatively prescribed requirements concerning the quantity and quality of evidence; and (2) a subjective criterion, reflecting the degree of internal conviction of the investigator, prosecutor, or court, formed on the basis of a comprehensive, complete, and impartial examination of all circumstances of the case. This combination of criteria ensures a balance between procedural requirements and the cognitive nature of evidentiary activity.

The amendments introduced to Part 4 of Article 99 of the Criminal Procedure Code of Ukraine have been positively assessed. According to these amendments, copies of information (including computer data) obtained by an investigator or prosecutor with the assistance of a specialist are recognized by the court as originals

of documents. This provision effectively legitimizes the application of forensic methods for copying digital data and means that if an investigator, with the participation of an information technology specialist, copies relevant files from a computer or another electronic system onto a separate storage medium, such a copy will possess the same evidentiary value as the original information carrier. Consequently, the legislator has departed from the mandatory requirement of seizing technical devices (servers, mobile devices, etc.) and has permitted the use of duly certified copies of electronic documents as sources of evidence, thereby maintaining an appropriate balance between the effectiveness of pre-trial investigation and the protection of property rights of device owners. At the same time, shortcomings of this legislative provision have been identified, namely the absence of a detailed procedure governing the inclusion, registration, and storage of such electronic evidence within criminal case files, as well as the lack of a clearly defined circle of responsible persons.

An algorithm for the seizure of digital storage media has been proposed, which includes: (1) taking measures to prevent any alteration of data after seizure (for example, disconnecting a computer from power, using write-blocking devices, placing a smartphone in a shielded container to block signals, etc.); (2) documenting all circumstances related to the seizure, including the time of seizure, persons having access, serial numbers of devices, the operational status of equipment (powered on or off), and the presence of passwords or encryption; and (3) immediate duplication of data (creation of a copy) in the presence of witnesses or through continuous video recording with the involvement of an IT specialist.

Attention is drawn to the gradual transformation of judicial practice concerning the use of electronic evidence in criminal proceedings—from perceiving it as a subtype of documentary evidence to recognizing it as an independent source of evidentiary information. The principal developments in judicial approaches to electronic evidence include: (1) the establishment of consistent criteria for assessing digital data (authenticity, integrity, relevance, and admissibility); (2) the expansion of the range of admissible electronic evidence, from surveillance camera recordings

to screenshots from messaging applications, GPS coordinates, and file metadata; and (3) the assessment of such materials on the basis of a presumption of reliability unless proven otherwise. At the same time, it is emphasized that the absence of a statutory definition of “electronic evidence” in the Criminal Procedure Code of Ukraine results in inconsistent application of this legal institution.

Keywords: evidence, admissibility of evidence, admissibility of evidence, electronic evidence, criminal proceedings, criminal process, electronic evidence.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, у яких опубліковано основні наукові результати дисертації:

1. Murzo Ye. O., Galchenko V. S. Electronic document as an object of forensic examination during the investigation of marauding. *Криміналістика і судова експертиза*. 2024. Вип. 69. С. 258–269. DOI: 10.33994/kndise.2024.69.24

2. Murzo Ye., Halchenko V. Electronic evidence as a means of proof during the pillage investigation. *Scientific Journal of the National Academy of Internal Affairs*. 2023. Vol. 28. No. 3. P. 48–57. DOI: https://doi.org/10.56215/naia-herald/3.2023.48

3. Гальченко В. С. Міжнародно-правовий досвід використання електронних доказів як засобу доказування у кримінальному провадженні. *Науковий вісник Дніпровського державного університету внутрішніх справ*. 2026. № 1. С. 269–274. DOI: https://doi.org/10.32782/2078-3566-2026-1-35

4. Гальченко В. С. Особливості доказування на підставі електронних доказів: судова практика. *Вісник Кримінологічної асоціації України.* 2026. Т. 38. № 1 (Part II). С. 386–396. DOI: https://doi.org/10.32631/vca.2026.1.p2.35

5. Гальченко В. С. Вилучення та процесуальне оформлення електронних доказів під час проведення досудового розслідування. *Вісник Кримінологічної асоціації України.* 2026. Т. 36. № 2 (Part I). С. 223–233. DOI: https://doi.org/10.32631/vca.2026.2.p1.17

Праці, які засвідчують апробацію матеріалів дисертації:

1. Гальченко В. С. Докази й доказування в кримінальному процесі під час дії воєнного стану. *Кримінальне судочинство: права людини під час дії надзвичайного або воєнного стану* : матеріали Міжнар. наук.-практ. конф. (Київ, 18 листоп. 2022 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2022. С. 218–220.

2. Гальченко В. С. Проблемні питання допустимості електронних доказів на досудовому слідстві. *Кримінальне судочинство: сучасний стан та*

перспективи розвитку : матеріали міжвідом. наук.-практ. конф. (Київ, 28 квіт. 2023 р.) / редкол.: С. С. Чернявський, Я. Ю. Конюшенко, В. В. Корольчук, Ю. В. Сухомлин. Київ : Нац. акад. внутр. справ, 2023. С. 43–46.

3. Гальченко В. С., Мурзо Є. О. Належність і допустимість електронних доказів, отриманих під час розслідування кримінального правопорушення за ст. 432 КК України. *Кримінальне процесуальне право на сучасному етапі розвитку України* : матеріали круглого столу, присвяч. 40-річчю кафедри крим. процесу (Київ, 27 жовт. 2023 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2023. С. 204–207.

4. Гальченко В. С. Електронні докази в кримінальному процесі. *Кримінальне судочинство: сучасний стан та перспективи розвитку* : матеріали Всеукр. наук.-практ. конф., присвяч. пам’яті проф. Ю. І. Азарова (Київ, 2 трав. 2024 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2024. С. 193–195.

ЗМІСТ

ВСТУП……... 18

РОЗДІЛ 1. ТЕОРЕТИЧНІ Й ІСТОРИЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНЕ ПРОЦЕСУАЛЬНЕ ЗАКОНОДАВСТВО……..... 28

1.1. Стан наукового дослідження електронних доказів у кримінальному провадженні……... 28

1.2. Співвідношення понять «оригінал», «копія» електронних доказів…… 44

1.3. Міжнародно-правовий досвід використання електронних доказів як засобу доказування в кримінальному провадженні……... 57

Висновки до розділу 1…….. 72

РОЗДІЛ 2. ПРАВОВІ ПІДСТАВИ ТА ПОРЯДОК ДОСЛІДЖЕННЯ ДОКАЗІВ З ПОЗИЦІЇ ЇХ НАЛЕЖНОСТІ Й ДОПУСТИМОСТІ….. 75

2.1. Належність електронних доказів у кримінальному провадженні…... 75

2.2. Допустимість електронних доказів у кримінальному провадженні……... 89

2.3. Взаємозв’язок допустимості й належності доказів і стандартів доказування…… 104

Висновки до розділу 2…….. 122

РОЗДІЛ 3. ПОРЯДОК ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ ТА СУДОВОГО ПРОВАДЖЕННЯ…… 126

3.1. Вилучення та процесуальне оформлення електронних доказів під час проведення досудового розслідування……. 126

3.2. Особливості доказування на підставі електронних доказів: судова практика……. 140
Висновки до розділу 3…….. 161

ВИСНОВКИ……. 165
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…… 172
ДОДАТКИ……. 191

ВСТУП

Обґрунтування вибору теми дослідження. Інформаційні технології зумовили необхідність у передачі даних, обміні інформацією. Розвиток інформаційних технологій своєю чергою актуалізує потребу належної правової регламентації електронного доказування. Такий підхід до врегулювання питання електронних доказів зменшить кількісні показники вчинення інформаційних злочинів і створить дієвий механізм реалізації відповідних прав та свобод усіх учасників кримінального провадження.

Доказами є показання, речові докази, документи, висновки експертів. Ці джерела доказів встановлюють наявність чи відсутність фактів й обставин, що мають значення для кримінального провадження та підлягають доказуванню. Будь-які відомості перед тим, як набути статусу доказів, мають бути оцінені з огляду на належність, допустимість, достатність і достовірність.

Докази в кримінальному провадженні передбачають процедуру збирання, фіксації та використання, порядок роботи з доказами прописано в законі, однак фіксацію їх електронного вигляду не відображено в Кримінальному процесуальному кодексі (КПК) України. Відсутність законодавчого регулювання може слугувати підставою для визнання електронних доказів недопустимими.

Згідно зі ст. 85, 86 КПК України, доказ визнають допустимим, якщо його отримано в порядку, встановленому КПК, і належним – якщо він прямо чи опосередковано підтверджує наявність чи відсутність обставин, що підлягають доказуванню в кримінальному провадженні, й інших обставин, які мають значення для кримінального провадження, а також достовірність чи недостовірність, можливість чи неможливість використання інших доказів.

Про наявність складнощів на практиці з визначенням процесуального статусу електронних даних як доказів зауважують опитані правозастосувачі (92,9 %). Крім того, на думку респондентів, причинами, які найчастіше

призводять до сумнівів стосовно допустимості електронних доказів є порушення порядку їх отримання (35,7 %); неможливість підтвердити автентичність даних (33,3 %); неналежна фіксація в протоколах процесуальних дій (31 %). Водночас у доктрині кримінального процесу, попри несформованість єдиного підходу до розуміння змісту електронних доказів, одностайно акцентовано на необхідності визначення в положеннях КПК України терміна «електронні докази», встановленні їхніх ознак, юридичних властивостей та способів закріплення. Пропозицію щодо запровадження окремої статті КПК України, яка містила б визначення поняття «електронні (цифрові) докази», схвалюють й опитані представники юридичної спільноти (97,6 %).

Аспекти належності й допустимості електронних доказів у кримінальному процесі України досліджували В. В. Вапнярчук, І. В. Гловюк, В. П. Гмирко, Г. Ф. Горський, Ю. М. Грошевий, Н. В. Друзенко, І. В. Жук, І. Г. Каланча, О. В. Капліна, С. О. Ковальчук, О. О. Костенко, О. В. Котенко, О. О. Куриляк, О. П. Кучинська, М. А. Макаров, М. М. Михєєнко, М. А. Погорецький, В. О. Попелюшко, С. М. Стахівський, О. В. Таран, Л. Д. Удалова, О. В. Угриновська, М. І. Хавронюк, В. Г. Хахановський, О. Ю. Хабло, С. С. Чернявський, В. І. Школьніков, О. Г. Шило, В. Ю. Шепітько, О. О. Юхно, які у своїх працях аналізували питання процесуального статусу електронних доказів, особливості їх збирання, фіксації, перевірки достовірності й оцінки в умовах цифровізації кримінального судочинства.

Водночас питання, пов’язані з використанням електронних доказів, зокрема в період активної цифровізації державницьких процесів і суспільного розвитку, дії правового режиму воєнного стану на території України, потребують уточнення в сучасних реаліях.

Науково-теоретичне підґрунтя дисертації становлять праці фахівців у галузі кримінального процесу, а також роботи із загальної теорії держави і права, кримінального права, криміналістики й інших галузевих правових наук, зокрема іноземних дослідників. Нормативною базою дисертації є Конституція

України, законодавчі акти України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, постанови Верховної Ради України, акти Президента України й Кабінету Міністрів України, нормативно-правові акти Міністерства внутрішніх справ (МВС) і Національної поліції України з приводу доказування на стадії досудового розслідування. Інформаційну базу дослідження становлять політико-правова публіцистика, проєкти нормативних актів, довідкові видання, статистичні матеріали діяльності правоохоронних органів і суду.

Отже, брак достатнього наукового підґрунтя, наявність прогалин у нормативно-правовому регулюванні належності й допустимості електронних доказів у кримінальному провадженні визначають актуальність дослідження зазначеної проблематики.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Тема дисертації відповідає Плану дій з реалізації Національної стратегії у сфері прав людини на 2021–2023 роки (розпорядження Кабінету Міністрів України від 23 червня 2021 року № 756-р), Національній стратегії у сфері прав людини (Указ Президента України від 24 березня 2021 року № 119/2021), Цілям сталого розвитку України на період до 2030 року (Указ Президента України від 30 вересня 2019 року № 722/2019), Стратегії розвитку Національної академії правових наук України на 2021–2025 роки, що затверджена постановою загальних зборів НАПрН України від 26 березня 2021 року № 12-21, а також тематиці наукових досліджень і науково-технічних (експериментальних) розробок на 2020–2024 роки (наказ МВС України від 11 червня 2020 року № 454/2020).

Тему дисертації затверджено Вченою радою Національної академії внутрішніх справ від 25 жовтня 2022 року (протокол № 14).

Мета і завдання дослідження. *Мета* дисертаційного дослідження полягає в тому, щоб на підставі теоретичних положень юридичної науки, норм законодавства України та практики його застосування визначити сутність й особливості належності і допустимості електронних доказів, на цій основі

сформулювати пропозиції та рекомендації щодо їх подальшого вдосконалення.

Поставлена мета зумовила необхідність виконання таких *завдань:*

– схарактеризувати стан наукового дослідження електронних доказів у кримінальному провадженні;

– висвітлити значення термінів «оригінал», «копія» електронних доказів;

– розглянути міжнародно-правовий досвід використання електронних доказів як засобу доказування в кримінальному провадженні;

– окреслити зміст належності електронних доказів у кримінальному провадженні;

– проаналізувати допустимість електронних доказів у кримінальному провадженні;

– визначити взаємозв'язок допустимості й належності доказів і стандартів доказування;

– дослідити процеси вилучення та процесуального оформлення електронних доказів під час проведення досудового розслідування;

– опрацювати судову практику щодо особливостей доказування на підставі електронних доказів.

Об'єкт дослідження – кримінальні процесуальні відносини, а також кримінальне процесуальне законодавство щодо реалізації належності й допустимості електронних доказів.

Предмет дослідження – належність і допустимість електронних доказів у кримінальному провадженні.

Методи дослідження. З огляду на мету й завдання дисертаційного дослідження, у роботі використано загальнонаукові та спеціальні методи вивчення концептуальних положень порушеної проблематики.

Логіко-семантичний метод застосовано для уточнення змісту таких категорій, як «електронний доказ», «цифровий слід», «матеріальний носій інформації», «копія електронних даних», що надало можливість визначити їх

співвідношення та функціональне навантаження в структурі доказування (підрозділи 1.1, 1.2). Історико-правовий метод дав змогу дослідити еволюцію правового регулювання електронних доказів у кримінальному процесі України, зокрема трансформацію підходів від фактичного ототожнення електронних даних із документами до поступового виокремлення їх як самостійного доказового явища, а також проаналізувати передумови впровадження новел Закону № 2137-IX (підрозділи 1.1, 2.1).

Методи класифікації та групування застосовано для систематизації видів електронних доказів, диференціації цифрових носіїв (смартфони, сервери, онлайн-акаунти, хмарні сервіси), визначення форм їх вилучення та копіювання, а також для структурування процесуальних механізмів отримання даних: обшуку, тимчасового доступу, тимчасового вилучення, експертного дослідження (підрозділи 1.2, 2.1, 3.1).

Порівняльно-правовий метод використано для зіставлення чинного українського законодавства з підходами Європейського Союзу (ЄС), Великої Британії та Сполучених Штатів Америки (США) щодо вимог до автентичності, цілісності й допустимості електронних доказів, зокрема шляхом аналізу принципів ACPO, положень Регламенту (ЄС) 2023/1543 і Директиви (ЄС) 2023/1544, на підставі чого окреслено напрями адаптації національного процесуального регулювання до сучасних європейських стандартів (підрозділи 1.2, 2.1, 3.1).

Системно-структурний метод уможливив комплексну характеристику інституту електронних доказів через взаємозв’язок його елементів – цифрової інформації, процесуальної форми її отримання і технічних гарантій цілісності. Застосування цього методу забезпечило обґрунтоване виокремлення ключових етапів роботи з електронними доказами (виявлення, вилучення, копіювання, фіксація, зберігання, дослідження) і дало змогу теоретично описати їх у структурі досудового розслідування та судового розгляду (підрозділ 3.1).

Техніко-криміналістичний метод залучено під час аналізу сучасних цифрових технологій, які застосовують для забезпечення автентичності електронних даних, зокрема хешування, створення цифрових образів, ведення журналів доступу (audit trail), ізоляції пристроїв від зовнішнього впливу. Його застосування надало можливість сформулювати критерії збереження цифрової цілісності та практичні рекомендації щодо процесуальної фіксації електронних доказів (підрозділ 3.1).

Наукова новизна отриманих результатів. На підставі теоретичних положень юридичної науки, норм законодавства України та практики його застосування в дисертації визначено сутність й особливості належності та допустимості електронних доказів, на цій основі сформульовано пропозиції та рекомендації щодо їх подальшого вдосконалення. У дисертації аргументовано положення, що становлять наукову новизну, а саме:

вперше:

– визначено необхідність законодавчого закріплення процесуального порядку фіксації вилучення, копіювання та отримання електронних (цифрових) даних шляхом складання протоколу, який повинен містити відомості про спосіб отримання електронних даних; технічні засоби, що використовували під час вилучення або копіювання; опис джерела отримання даних; цифрові ідентифікатори та контрольні хеш-значення електронних даних; інші відомості, необхідні для підтвердження цілісності й автентичності даних. У зв’язку з цим сформульовано пропозиції про доповнення КПК України окремою статтею;

– обґрунтовано підхід, згідно з яким електронні (цифрові) докази визнають належними й допустимими, якщо з огляду на їх вид (абонентські, трафік-, контент-дані) вони прямо або опосередковано підтверджують чи спростовують обставини, що підлягають доказуванню, й отримані в обсязі, необхідному та достатньому для досягнення мети кримінального провадження;

– доведено, що протокол процесуальної дії щодо вилучення електронних доказів (огляд, обшук, тимчасовий доступ до речей і документів тощо) обов'язково має містити опис системи, доступ до якої отримано, способу доступу до неї, застосованих програм/інструментів, хеш-значення, тайм-стемпів; журнал дій слідчого або спеціаліста, залученого до проведення такої дії;

– з позиції допустимості електронних доказів у кримінальному провадженні виокремлено їхні специфічні риси: 1) фізичне існування електронного документа неможливе поза межами носія інформації, тому для забезпечення достовірності доказу необхідно ідентифікувати носій, ураховуючи його тип, модель й індивідуальні машинні характеристики; 2) мають нематеріальний характер, що унеможливлює їх безпосереднє сприйняття без застосування відповідних програмно-технічних засобів і спеціального інструментарію; 3) можуть бути змінені, пошкоджені або знищені в процесі експлуатації пристрою користувачем чи під впливом фізичних чинників; 4) за стадіями виготовлення документи, зокрема електронні, поділяють на оригінали, дублікати, копії та виписки, водночас позначення «оригінал», «дублікат», «копія» є умовними, тому що в усіх цих випадках електронний документ залишається оригіналом;

удосконалено:

– позицію, відповідно до якої електронні докази слід тлумачити як інформацію в електронній (цифровій) формі, що містить відомості про обставини, які підлягають доказуванню в кримінальному провадженні, до яких належать такі види електронних даних: абонентські дані; трафік-дані; контент-дані. У зв'язку з цим сформульовано пропозиції про доповнення КПК України окремою статтею;

– твердження про те, що належне функціонування інституту електронних доказів передбачає створення та впровадження технічних й організаційно-правових стандартів інформаційно-телекомунікаційної системи досудового розслідування, які забезпечуватимуть збереження автентичності

даних, що є необхідною організаційно-правовою передумовою з конкретним кримінально-процесуальним ефектом;

– позицію про трирівневу належність електронних доказів, яка охоплює технічний, процесуальний та інформаційний рівні релевантності, що усуває обмеженість класичної моделі належності й допустимості як «зв'язок між доказом і фактом», адаптує її до цифрової реальності, у якій електронний доказ відображає не фізичний об'єкт, а інформаційний факт, зафіксований у цифровому середовищі;

– тлумачення термінів «електронний доказ» і «електронний документ» в тій частині, що усуває їх ототожнення як на стадії досудового розслідування, так і під час судового розгляду, дає змогу визнати джерелом доказу не лише документи із цифровими підписами, а й лог-файли, метадані, контент і трафік, дані відповідних пристроїв тощо;

дістало подальший розвиток:

– підходи до імплементації в національне законодавство актів права Європейського Союзу (Регламент (ЄС) 2023/1543, Директива (ЄС) 2023/1544) і використання їх як аксіологічних орієнтирів для формування національної доктрини електронних доказів, оскільки вони містять універсальні стандарти пропорційності, категоризації даних, гарантій захисту прав людини та процедурної легітимності;

– характеристика проблемних питань використання електронних доказів у кримінальному процесуальному праві України, серед яких: невідмежованість електронного доказу від інших джерел доказів; невизначеність джерел одержання електронних доказів у кримінальному провадженні; недостатність нормативно-правового регулювання щодо застосування копії електронних доказів, оригінали яких утрачено; обмеження можливостей дізнавача стосовно застосування електронних доказів тощо;

– позиція щодо необхідності законодавчого закріплення детальної процедури долучення, реєстрації та зберігання електронних доказів у

матеріалах кримінального провадження з визначенням кола відповідальних осіб;

– напрями подальших наукових досліджень, що спрямовані на формування цілісної кримінальної процесуальної концепції електронних доказів із чітким розмежуванням інформаційного й матеріального компонентів доказування (метадані, цифрові події, лог-файли тощо як самостійні джерела доказів).

Практичне значення одержаних результатів полягає в тому, що вони становлять як науково-теоретичний, так і практичний інтерес, а саме:

– низка пропозицій можуть доповнити нормативно-правові акти, а також законопроєкти, які знаходяться на розгляді у Верховній Раді України й стосуються особливостей використання електронних доказів у кримінальному провадженні з позицій їх належності та допустимості;

– сформовані пропозиції та рекомендації щодо використання електронних доказів у кримінальному провадженні з позицій їх належності й допустимості використовують у діяльності органів досудового розслідування Національної поліції України (акт впровадження Головного слідчого управління Національної поліції України від 9 липня 2025 року № 65345-2025);

– наукові рекомендації та висновки можуть бути використані для створення теоретико-методологічної бази вдосконалення інституту електронних доказів у кримінальному провадженні з позицій їх належності й допустимості;

– матеріали використовують в освітньому процесі під час викладання спеціалізованих дисциплін кримінального процесуального спрямування.

Особистий внесок здобувача. Сформульовані в дисертаційному дослідженні висновки та рекомендації визначають наукову новизну дослідження та розроблені відповідно до вимог законодавства України, норм і стандартів академічної доброчесності з метою поглибленого аналізу наукових категорій, комплексного дослідження основних правових елементів

належності й допустимості електронних доказів у кримінальному провадженні.

Апробація матеріалів дисертації. Ключові положення дисертації, висновки й рекомендації оприлюднено на міжнародних, всеукраїнських і регіональних науково-практичних конференціях, засіданнях круглих столів і семінарів, серед яких: Міжнародна науково-практична конференція «Кримінальне судочинство: права людини під час дії надзвичайного або воєнного стану» (м. Київ, 18 листопада 2022 року); міжвідомча науково-практична конференція «Кримінальне судочинство: сучасний стан та перспективи розвитку» (м. Київ, 28 квітня 2023 року); круглий стіл, присвячений 40-річчю кафедри кримінального процесу (м. Київ, 27 жовтня 2023 року); Всеукраїнська науково-практична конференція, присвячена пам'яті професора Ю. І. Азарова (м. Київ, 2 травня 2024 року); проходження програми «Використання цифрової інформації у кримінальному процесуальному доказуванні» з отриманням сертифіката № 100088 від 1 червня 2023 року.

Публікації. За результатами дослідження опубліковано п'ять статей у наукових фахових виданнях України, а також чотири тези доповідей на наукових конференціях, зокрема міжнародних.

Структура та обсяг дисертації. Дисертація складається з анотації, вступу, трьох розділів, що містять вісім підрозділів, висновків, списку використаних джерел (163 найменування на 19 сторінках) і чотирьох додатків (на 17 сторінках). Повний обсяг дисертації становить 207 сторінок, із них обсяг основного тексту – 155 сторінок.

РОЗДІЛ 1
ТЕОРЕТИЧНІ Й ІСТОРИЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНЕ ПРОЦЕСУАЛЬНЕ ЗАКОНОДАВСТВО

1.1. Стан наукового дослідження електронних доказів у кримінальному провадженні

Стрімка цифровізація суспільного життя зумовлює нові виклики для кримінальної юстиції. Злочинність дедалі частіше пов’язана з використанням комп’ютерних технологій, а відповідні особи залишають після себе специфічні електронні сліди – зміни в цифровому середовищі, що не мають матеріального вираження в традиційному значенні. Такі сліди злочину не відповідають усталеним класифікаціям доказів і потребують нових підходів до їх виявлення, фіксації та використання в доказуванні. Тож виникла концепція електронних доказів – окремої категорії доказів, пов’язаних із цифровою інформацією. Проте на теоретичному й законодавчому рівні ця категорія досі залишається недостатньо визначеною, що ускладнює ефективне використання відповідних даних у кримінальному провадженні.

Відповідаючи на виклики цифрової доби, український законодавець упровадив поняття електронних доказів у суміжних процесуальних галузях ще 2017 року [88]. Зокрема, зміни до Цивільного процесуального кодексу (ЦПК), Господарського процесуального кодексу (ГПК) та Кодексу адміністративного судочинства (КАС) України передбачили наявність електронних доказів як самостійного інструменту доказування [44]. У цих актах електронними доказами визначено інформацію в електронній (цифровій) формі, що містить дані про обставини справи, наприклад, електронні документи (текстові, графічні зображення, фотографії, відео- та звукозаписи тощо), вебсайти, повідомлення (текстові, мультимедійні, голосові), метадані, бази даних та інші

дані в електронній формі. Електронні докази поряд із речовими та письмовими прямо визнані окремим видом доказів (п. 1 ч. 2 ст. 76 ЦПК України) із визначенням порядку їх подання, дослідження, зберігання та повернення. Запровадження цих новел отримало загалом позитивні відгуки науковців і практиків, а також посилило інтерес дослідників до проблематики електронних доказів [44].

Слід також акцентувати на позиції, яку обстоюють А. В. Гутник й А. Я. Хитра в монографії «Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні». У цій монографії автори системно аналізують проблематику використання електронних документів у кримінальному провадженні, поєднуючи теоретичний (кримінально-процесуальний) і криміналістичний аспекти. Вони розпочинають з аналізу сучасного стану наукових досліджень, пропонують визначення поняття електронного документа в системі джерел доказів, класифікують електронні документи за різними ознаками й досліджують нормативно-правову базу та міжнародний досвід. Друга частина окреслює кримінально-процесуальні засади (належність, допустимість, достовірність) електронних документів, а третя – криміналістичні (способи збирання, дослідження, міжнародні підходи). За результатами дослідження сформульовано низку практичних рекомендацій для вдосконалення правозастосування в Україні [27].

У кримінальному процесі України процес нормативного врегулювання електронних доказів потребує активізації. Кримінальний процесуальний кодекс досі не виокремлює доказів в електронній формі як окремої категорії: їх фактично розглядають крізь призму документів, до них застосовують загальні правила доказування [111]. Утім деякі положення вже передбачено, зокрема електронний документ визнано одним із можливих процесуальних джерел доказів (ч. 1 ст. 99 КПК України) нарівні з іншими документами [44]. Доказами можуть бути матеріали фото-, відеозйомки, звукозапису й інші носії інформації (зокрема електронні), а оригіналом електронного документа є його

відображення (копія), яка має таку саму силу, як оригінал. Крім того, КПК допускає фіксацію окремих слідчих дій в електронній формі (наприклад, відеозапис під час обшуку чи допиту, додавання електронних носіїв до протоколів слідчих дій за ст. 104, 105 КПК) і проведення дистанційних процесуальних дій (допит, впізнання через відеоконференцію тощо) [53]. Однак ці норми не становлять цілісної системи регулювання електронних доказів і не враховують усіх специфічних властивостей цифрової інформації.

Крім цього, В. В. Романюк у статті «Критерії допустимості цифрових (електронних) доказів у кримінальному процесі» зосереджує увагу на систематизації критеріїв допустимості електронних доказів у кримінальному процесі України. Автор виокремлює такі основні критерії: належне джерело отримання доказів; належний суб'єкт доказування; належний спосіб збирання доказів. Також проаналізовано відповідну судову практику та доктринальні підходи, виявлено прогалини в правовому регулюванні та сформовано пропозиції для їх подолання (передусім через чітке визначення процедур збору та зберігання електронних доказів) [85].

У науковій статті О. П. Метелева висвітлено проблемні аспекти належності й допустимості цифрових доказів у кримінальному провадженні. Учений доводить, що традиційні процесуальні категорії (належність, допустимість, достовірність) не цілком ураховують специфіку цифрових слідів, електронних носіїв і метаданих, тому застосування таких доказів у практиці є ускладненим. Автор акцентує на необхідності гармонізації кримінального процесуального законодавства із сучасними інформаційно-технологічними викликами, а саме: модифікації процедур вилучення та фіксації цифрових даних, підвищенні експертно-технічної спроможності, а також визначенні чіткого механізму оцінки таких доказів [62].

В цьому контексті заслуговує на увагу дисертаційне дослідження І. Г. Каланчі, яка серед іншого розробила комплекс алгоритмів, що пропонується як три стратегії фіксації доказів електронної форми у кримінальному процесі України: фізичне вилучення електронних носіїв

інформації або комп'ютерних систем; огляд та копіювання комп'ютерних даних; огляд та фіксація інформації з відкритих джерел [36].

Суттєвим зрушенням стало ухвалення Закону від 15 березня 2022 року № 2137-IX, яким внесено зміни до КПК у частині збирання та використання електронних даних. Цей Законом уточнює низку термінів і процедур, зокрема: замінено словосполучення «носії комп'ютерної інформації» на «носії комп'ютерних даних», визначено, що дублікати електронних документів визнають оригіналами [23], а також урегульовано можливість створення процесуальних рішень в електронній формі з накладенням електронного підпису посадової особи [23]. Запроваджені зміни суттєво покращили нормативну базу доказування із застосуванням електронних доказів [88]. Водночас залишаються невирішеними окремі питання, які потребують подальшого врегулювання для повноцінного й ефективного застосування нових норм на практиці [88]. Зокрема, проблема полягає в тому, що чинна редакція ст. 99 КПК досі прив'язує поняття документа до матеріального носія інформації [44]. Такий підхід не враховує природи електронних файлів, які можуть одночасно зберігатися в хмарних системах, на декількох пристроях чи міститися в пам'яті зі значним масивом інших даних [44]. Тому виникають складнощі під час вилучення інформації, розміщеної на віддалених серверах або в мережі Інтернет, куди органи досудового розслідування не мають прямого доступу [44]. У судовій практиці акцентують, що ототожнення електронного доказу із фізичним носієм є неправомірним, оскільки відмітною рисою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія. Верховний Суд зауважив, що електронна форма доказу не може бути підставою для визнання його недопустимим, а однакові екземпляри електронного документа на різних носіях слід розглядати як рівноцінні оригінали. Тож постала необхідність внести до КПК України комплексні зміни, що закріплять електронні (цифрові) докази як окремий вид доказів у кримінальному провадженні, визначивши їх статус і порядок поводження з ними.

У науковій літературі не сформованого єдиного підходу до дефініції та природи електронних доказів. Термін тлумачать по-різному: поряд із поняттям «електронні докази» часто використовують термін «цифрові докази», їх переважно трактують як синоніми [111]. Чимало авторів також оперує суміжними поняттями – «електронний документ», «електронні (цифрові) сліди», «електронні відображення» тощо. Технічно ж коректнішим деякі дослідники вважають поняття «цифровий доказ», адже йдеться про інформацію, подану в числовій (дискретній) формі [111]. Водночас будь-який електронний доказ фактично є цифровим, оскільки або створений у цифровому форматі, або згодом перетворений у нього [111]. Тож терміни «електронний» і «цифровий» доказ розглядають як рівнозначні, хоча питання термінології лишається дискусійним.

Ще одним вагомим напрацюванням у цьому напрямі є стаття А. В. Коваленка «Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання», у якій автор здійснює огляд наукових і нормативно-правових підходів до категорії «електронні докази» в українському кримінальному провадженні. У публікації висвітлено поняття «цифрові джерела інформації», «електронні сліди», «електронні документи», тож констатовано, що категорія електронних доказів ще недостатньо теоретично і практично унормована. Автор також окреслює перспективи використання електронних доказів, акцентує на потребі в адаптації процесуальних норм, удосконаленні процедур збору й аналізу цифрової інформації, а також у підготовці спеціалізованих криміналістичних засобів для її перевірки [44].

Крім цього, питання цифрового доказування у своїх працях розглядали також О. І. Гарасимів, С. І. Марко, О. В. Ряшко. Автори у статті аналізують тенденцію зростання рівня злочинності, пов’язаної з ІТ-технологіями, розглядають виклики, що створюють цифрові докази для кримінального провадження. Вони доводять, що брак єдиного понятійного апарату й стандартизованих процедур для обробки цифрових доказів ускладнює їх

використання в судочинстві. Дослідники значущими визначають такі проблеми: двозначність у законодавстві щодо поняття електронних документів, несформованість чітких критеріїв достовірності цифрових доказів, недостатній рівень технічного й методичного забезпечення збирання та оцінки таких доказів [21].

Сучасна доктрина пропонує кілька основних підходів до тлумачення сутності електронних доказів. Перший підхід можна назвати інформаційним: більшість учених вважає, що електронні докази – це дані (інформація), що виникли внаслідок використання комп'ютерної техніки й можуть бути використані в судовому процесі [111]. Відповідно до цього підходу електронний доказ ототожнюють з інформацією (відомостями), зафіксованою у цифровій формі, яка має значення для справи. Другий підхід – об'єктний: деякі дослідники пропонують розглядати електронні докази як об'єкти цифрового (електронного) середовища, що можуть містити інформацію, важливу для кримінального провадження. Тут акцентовано, що носієм доказової інформації є нематеріальний об'єкт – файл, електронний запис, тобто елемент віртуального простору. Третій підхід – комплексний (технологічний): згідно з ним електронним доказом є будь-який доказ, отриманий з даних, що містяться в будь-якому пристрої або генеруються таким пристроєм, функціонування якого залежить від програмного забезпечення чи даних, що зберігають або передають через комп'ютерну систему чи мережу. Таке широке трактування фактично охоплює всі можливі цифрові дані, пов'язані із функціонуванням електронних пристроїв, й акцентує на технологічній природі походження доказів.

Окрім змістового визначення, дискусійним є питання про місце електронних доказів серед традиційних процесуальних категорій доказів і джерел доказів. Деякі науковці уникають терміна «електронні докази» через його новизну. У сфері цивільного процесу А. Каламайко (2016) використовував поняття «електронні засоби доказування» замість електронних доказів, ставлячи їх на один рівень із письмовими доказами [44].

У криміналістиці пропонують використовувати поняття «електронний (цифровий) слід». Згідно з визначенням Г. Авдєєвої та С. Стороженка, електронні цифрові сліди – це матеріальні невидимі сліди, що можуть бути виявлені, зафіксовані й досліджені за допомогою цифрових пристроїв і містять криміналістично значущу інформацію в електронно-цифровій формі на матеріальних носіях.

Слід акцентувати на напрацюваннях В. В. Вапнярчука, який у своєму дисертаційному дослідженні «Теоретичні основи кримінального процесуального доказування» здійснив фундаментальний теоретико-правовий аналіз інституту доказування в кримінальному процесі, зосередивши увагу на розмежуванні понять «належність» і «допустимість» доказів. Автор доводить, що сучасні інформаційні технології створюють нові види джерел доказів, які потребують спеціального процесуального врегулювання. У дослідженні простежено еволюцію доктрини доказування, класифіковано види доказів, запропоновано вдосконалення критеріїв їх оцінки в умовах цифровізації судочинства. Ці положення стали основою для подальших досліджень електронних доказів в Україні [9].

Паралельно деякі вчені ввели в обіг термін «електронне відображення» стосовно електронних даних. Зокрема, Ю. Орлов і С. Чернявський вважають електронні відображення різновидом джерел доказів і пропонують ототожнювати цей термін із поняттям електронного документа [67]. Інші фахівці піддали сумніву коректність такого терміна, адже поняття «відображення» в криміналістиці традиційно використовують у контексті механізму утворення слідів і вказує на двосторонню взаємодію об’єктів [44]. На думку А. Коваленка, використовувати поняття «електронне відображення» слід як синонім «електронного сліду», а не електронного документа [44]. Справді, електронний документ як вид документа має низку формальних реквізитів і структуровану форму подання, що не притаманно просто сліду. Отже, питання термінології залишається відкритим: різні наукові школи

пропонують власний понятійний апарат для опису цифрових доказів, що свідчить про етап становлення теорії електронних доказів.

Також слід виокремити напрацювання Р. Благути, який у статті «Використання електронних доказів у кримінальному процесі України» розглядає електронні докази з позиції євроінтеграційних процесів і порівняльного права. Публікація окреслює сучасний стан нормативної бази України у сфері цифрових доказів, порівнює її з положеннями Будапештської конвенції та практикою держав ЄС. Автор зауважує, що українська судова практика лише формує підходи до автентифікації електронних матеріалів, а ключовим викликом є забезпечення «ланцюга збереження» (chain of custody). Автор пропонує адаптацію європейських стандартів e-evidence у національне кримінальне процесуальне законодавство [127].

Слід зазначити, що українські автори загалом виважено впроваджують категорію «електронні докази» у кримінально-процесуальну лексику. Зокрема, В. Мурадов констатує необхідність суттєвого вдосконалення методики збирання та дослідження електронних доказів як на досудовому слідстві, так і в судовому розгляді, хоча власного визначення цього терміна не пропонує. Д. Алєксєєва-Процюк та О. Брисковська пропонують визначення електронних доказів як фактичних даних, що зберігаються в електронному вигляді на будь-яких видах носіїв і стають доступними для сприйняття людиною після обробки спеціальними технічними засобами та програмним забезпеченням [1]. Вони акцентують на необхідності законодавчого врегулювання як термінології, так і класифікації електронних доказів. Д. Цехан використовує термін «цифрові докази», посилаючись на англомовний термін «digital evidence», який активно використовують за кордоном [114]. На його думку, цифрова інформація нині не відповідає жодній з наявних груп класифікації доказів, тому слід увести до наукового та законодавчого обігу окрему категорію цифрового доказу, який слід трактувати як фактичні дані в цифровій формі на будь-якому типі носія, що стають доступними для

сприйняття після обробки ЕОМ і на підставі яких слідчий, прокурор чи суд встановлюють обставини, що мають значення для провадження.

М. Шумило, Р. Юрка, О. Капліна у статті «Інформаційна теорія доказів і проблеми використання електронних засобів у доказуванні» зауважують, що дослідження пропонує застосування інформаційної теорії доказів до аналізу цифрових даних. Автори розглядають електронний доказ як носій інформації, що потребує спеціальних процедур фіксації, збереження та перевірки достовірності. У статті запропоновано концепцію «інформаційної цілісності доказу», що поєднує процесуальні й технічні вимоги. Також визначено роль експерта-криміналіста в оцінюванні достовірності електронних слідів і необхідність закріплення в КПК норм про спеціальні електронні протоколи [122].

Отже, наукові дослідження останніх років пропонують різні теоретичні моделі електронних доказів. Попри розбіжності в термінології, більшість авторів сходяться на думці, що електронні докази мають особливу природу, відмінну від традиційних речових чи письмових доказів, і тому потребують спеціального підходу до їх ідентифікації та оцінки. Ця особливість зумовлює необхідність розглядати електронні докази як самостійну категорію джерел доказів, яку поступово реалізують у наукових публікаціях і рекомендаціях.

Аналіз стану нормативної бази та літературних джерел засвідчує, що теорія і практика використання електронних доказів у кримінальному процесі знаходяться на етапі становлення. Нинішній рівень законодавчого врегулювання та наукової розробленості не цілком відповідає потребам практики. Правоохоронні органи постають перед низкою проблем під час роботи із цифровими доказами. Наприклад, брак чіткого визначення статусу електронної інформації в КПК призводить до того, що слідчим доводиться де-факто відносити цифрові дані до традиційних категорій (найчастіше – до речових доказів або документів), аби легітимно їх залучити до матеріалів справи. Досліджуючи проблему речових доказів, І. Крицька акцентує на проблемності віднесення цифрової інформації до цієї категорії та пропонує на

практиці визнавати цифрові носії інформації саме речовими доказами, з огляду на наявні законодавчі норми [54]. Такі рішення є вимушеними й не вирішують концептуальних прогалин.

Слід також зауважити, що аналітичні матеріали Верховного Суду (2025) «Практика оцінки відео- та електронних даних як доказів» містять узагальнення судових рішень стосовно допустимості електронних доказів: відеозаписів з камер спостереження, скриншотів, електронного листування, даних з мобільних телефонів тощо. Суд констатує, що такі докази підлягають оцінці за загальними правилами доказування, але мають бути перевірені на предмет автентичності та належного джерела походження. Виокремлено важливість процесуального оформлення вилучення цифрових носіїв і надання висновків спеціалістів, а також недопустимість доказів, здобутих із порушенням правил доступу до інформаційних систем. У документі окреслено орієнтири для судів нижчих інстанцій щодо кваліфікації таких доказів [154].

Сучасний стан наукового розроблення електронних доказів вирізняється переходом від переважно описового аналізу феномену електронних доказів до проблемно орієнтованих і методологічних студій: акцент зміщується на критерії допустимості, формування національних стандартів збору, автентифікації та збереження (chain of custody), а також на інтеграцію порівняльно-правових імпульсів із права ЄС (e-Evidence Package) у кримінальне процесуальне мислення України. Наукові публікації та судово-освітні заходи дедалі частіше пов’язують осмислення електронних доказів із практичними викликами воєнного часу (документування воєнних злочинів, кіберінциденти, використання OSINT) і посиленням ролі судової практики як «каталізатора» доктринальних корекцій [156].

Актуальні публікації окреслюють кілька стабільних кластерів: (a) дефініція та місце електронних (цифрових) доказів у системі джерел; (b) критерії допустимості й достовірності; (c) способи збирання і документування (включно з копіюванням та форензичним збереженням); (d) класифікація та джерела походження (офіційні установи, автономні

системи, користувацький контент, провайдери, відкриті джерела); (e) міжнародне співробітництво і транскордонний доступ; (f) права людини й баланс із процесуальною економією; (g) імплементація пакета e-Evidence та адаптація до нових строків його застосування і транспозиції. Таке багатошарове структурування відображає перехід від дискусій про «новаційність» категорії до програмування стандартизованих процедур [2].

Л. М. Ніколенко в роботі «Використання електронних доказів в кримінальному процесі зарубіжних країн» аналізує особливості використання електронних доказів у кримінальному процесі зарубіжних країн. Зазначено, що на теперішній час електронні докази стали незамінними для кримінальних розслідувань і судових процесів у світі. Увагу сфокусовано на важливості правового регулювання кримінально-процесуальної форми цифрових технологій. Неналежний характер такого регулювання тягне за собою певні правові наслідки, зокрема визнання електронних доказів неналежними або недопустимими. Проаналізовано досвід деяких іноземних країн у сфері визнання та використання електронних доказів (США, Великої Британії, Китайської Народної Республіки та країн Європейського Союзу). Доведено, що кожна держава обирає власний шлях і підхід до включення таких доказів у свої правові системи залежно від правових традицій, технологічної інфраструктури та міркувань конфіденційності. На підставі аналізу процесуальних кодексів констатовано, що процесуальна наука розробляє теорію щодо електронних доказів за галузевим принципом. Зауважено, що їх основою є загальні цифрові технології, тому це надає можливість розробити єдині міжгалузеві правила використання електронних доказів у будь-якому процесі. Визначено, що в англосаксонській правовій системі немає чіткого розмежування доказів на види. Доказове право будується на типових проблемних ситуаціях. Проаналізовано законодавство США, яке регулює використання електронних доказів у кримінальному процесі [66].

Також простежується прагнення до уніфікації понятійного апарату, зокрема щодо термінів «електронні докази» і «цифрові докази», причому

відхід від жорсткої прив’язки до матеріального носія актуалізується під впливом судових позицій та європейських регулятивних актів. Авторські дефініції часто охоплюють критерії структурованості даних, їх форензичної відтворюваності та можливості верифікації (хеш-значення, журнали системних подій). Європейські інструменти (Regulation (EU) 2023/1543; Directive (EU) 2023/1544) опосередковано сприяють стандартизації, закладаючи поняттєву рамку «production/preservation orders» як процесуальних форм доступу до цифрових даних, що проєктується в національні дискусії про структуру джерел доказової інформації [2].

Автори пропонують ієрархічні класифікації джерел електронних доказів за ознакою первинності й умов доступу: офіційні установи/провайдери; автономні технічні системи (камери, реєстратори, датчики); користувацькі пристрої; відкриті вебресурси й соціальні медіа (OSINT); хмарні середовища. Це відображає прагнення усунути стихійний підхід до віднесення даних, який передбачає, зокрема, що до кожної групи можуть застосовувати диференційовані процесуальні гарантії (різні рівні судового контролю, технічна експертиза, ступінь інвазивності). Такі типології підживлюють подальші пропозиції закріпити в кримінальному процесуальному законодавстві модель класифікаційної рамки не лише за формою (документ/річ), а й за джерелом технологічного походження [63].

Західні аналітичні огляди виявляють «ахіллесову п’яту» нового режиму – фрагментарну відповідальність провайдерів і неоднорідність механізмів контролю на рівні держав-членів, що може створити асиметрію в доступі до даних і процесуальних гарантіях. Ці зауваги резонують з українським дискурсом про необхідність синхронізації внутрішніх процесуальних вимог (оформлення запитів, верифікація отриманих даних) з майбутніми стандартами direct cooperation. Отже, критика слугує превентивним інструментом для уникнення реплікації виявлених у ЄС вразливостей [137].

Оприлюднені судові аналітичні огляди та виступи суддів ВС 2024–2025 років функціонально компенсують брак кодифікованої секції в КПК

щодо електронних доказів, формуючи «soft law» орієнтири: визнання множинності еквівалентних носіїв, неприйнятність формального ототожнення носія та змісту, вимоги до відтворюваності процесуальних дій і релевантності технічних довідок спеціаліста. Це сприяє поступовій доктриналізації критеріїв, які потім цитують у наукових статтях як аргументативне підґрунтя реформ [107].

Науковий дискурс інтегрує аналіз новел щодо електронних комунікацій, змін до механізмів тимчасового доступу/вилучення в контексті переходу від матеріалізованого до датацентричного (data-centric) підходу. Так виникає ідея передбачити в КПК окрему главу або системний блок щодо електронних доказів, що міститиме: легальне визначення; правила диференційованого доступу; процедури створення дублікатів; стандарти технічної документації; особливості транскордонного запиту електронних даних. Методологічні публікації підкріплюють цю ідею аргументами про зменшення колізій та підвищення рівня передбачуваності правозастосування [131].

Деякі науковці порушують питання застосування алгоритмічного аналізу (розпізнавання облич, аналіз мережевої активності, класифікація великих масивів повідомлень) як допоміжного інструменту виокремлення релевантних фрагментів даних. Виклик полягає в презумпції «прозорості алгоритму»: у якому обсязі сторони повинні мати доступ до технічної документації або статистичних показників помилок, щоб забезпечити змагальність і можливість спростування. Дискусія корелює з європейськими занепокоєннями щодо фундаментальних прав у новому режимі e-Evidence, зокрема пропорційності масового вилучення даних і можливого «функціонального зсуву» приватних провайдерів у напрямі квазідержавних акторів [155].

Попри відчутний прогрес, зберігаються прогалини, серед яких: (a) відсутність уніфікованого процедурного стандарту вилучення та копіювання (chain of custody); (b) нечіткі критерії релевантності й мінімальної достатності (threshold) для масивів великих даних; (c) неформалізований

статус OSINT й автоматично зібраних даних; (d) неврегульований баланс між швидкістю транскордонних запитів (майбутні European Production/Preservation Orders) і захистом персональних даних; (e) недостатня методологія оцінювання ризиків маніпуляції deepfake/AI-генерованих артефактів у кримінальному процесі. Подальші дослідження мають поєднати компаративний аналіз (ЄС, США, Велика Британія) з емпіричними кейс-стаді (українські вироки, де ключову роль відіграв цифровий масив), щоб розробити доказово підтверджені рекомендації для кодифікації [132].

Через технологічні особливості електронних доказів постають складнощі із забезпеченням їх автентичності, цілісності й допустимості в суді. Будь-які зміни цифрових даних складно відстежити без спеціальних засобів, тому постає необхідність довести, що поданий електронний файл не був модифікований. Для гарантування достовірності нерідко залучають експертів із цифрової криміналістики або застосовують криптографічні засоби (хешування, електронний підпис тощо). Однак процесуальні процедури фіксації, вилучення і дослідження електронних доказів поки що недостатньо детально регламентовані, що може призводити до втрати інформації чи визнання доказів недопустимими. Брак спеціальних норм, адаптованих під цифрові реалії, спонукає судову практику напрацьовувати власні підходи: наприклад, Верховний Суд уже роз’яснив критерії допустимості електронного документа й визнав, що електронна форма не може бути причиною для відмови в доказуванні. Проте такі роз’яснення мають фрагментарний характер. Необхідним є системне вирішення – запровадження в законодавстві чітких правил збирання, перевірки й оцінки цифрових доказів, включно з процедурою документування дій з електронною інформацією.

Ще одним проблемним аспектом є барк єдиних стандартів класифікації та використання електронних доказів. Тривають дискусії, до якого саме процесуального джерела відносити дані в електронній формі [111]. Одні фахівці вважають, що всі електронні докази по суті є документами (оскільки містять інформацію), інші ж акцентують на їхній нематеріальній природі,

пропонуючи відокремити їх від документів і речей. Вирішення цього питання матиме практичні наслідки: від нього залежить, які процесуальні вимоги застосовувати (наприклад, щодо зберігання оригіналів, засвідчення копій, повернення носіїв тощо). Поки питання лишається відкритим, у правозастосуванні можливі різночитання і зловживання. Тож постала потреба в розробленні уніфікованої доктрини електронних доказів, яка була б закріплена в законі й деталізована в підзаконних актах або роз'ясненнях.

Перспективи використання електронних доказів безпосередньо пов'язані з подальшим розвитком правового регулювання та наукових рекомендацій. На міжнародному рівні напрацьовують досвід, корисний для України. Зокрема, країни Європейського Союзу, США, Великої Британії, Китай уже сформували певні рішення щодо проблеми цифрових доказів [88]. У ЄС 2023 року ухвалено спеціальні регламенти, спрямовані на уніфікування процедури отримання електронних доказів у транскордонних випадках [88]. Вони передбачають створення правових механізмів для швидкого отримання даних від провайдерів, спрощення співпраці між державами та забезпечення гарантій захисту даних. Для України, яка обрала курс євроінтеграції, важливо врахувати ці стандарти: імплементація підходів, визначених актами ЄС, є одним із завдань наближення національного законодавства до acquis ЄС. В умовах війни та зростання рівня кіберзлочинності Україна відчуває нагальну потребу посилювати власну спроможність протидіяти кіберзагрозам, що передбачає і вдосконалення механізмів роботи з електронними доказами.

Отже, сучасний стан наукового дослідження електронних доказів у кримінальному провадженні відображає перехідний етап – від усвідомлення проблеми до пошуку конкретних рішень. На порядку денному постало завдання сформулювати чітке науково обґрунтоване визначення електронних доказів та їх різновидів, розробити типові методики роботи з ними (вилучення, збереження, аналіз, презентація в суді) і закріпити ці напрацювання в нормативних актах. Тільки за умови поєднання зусиль наукової спільноти й

законодавця вдасться створити ефективну систему використання електронних доказів, що відповідатиме потребам правозастосування в цифрову епоху.

На підставі здійсненого аналізу можна дійти проміжних висновків. Законодавче поле потребує оновлення в контексті реалій цифрової доби. Кримінальний процесуальний кодекс України досі не містить визначення електронних доказів і спеціальних правил роботи з ними. Хоча 2022 року реалізовано перші кроки щодо врахування електронних даних у доказуванні (уточнено термінологію, визнано дублікат е-документа оригіналом тощо), цього недостатньо для подолання всіх проблем практики. Необхідно нормативно закріпити власне поняття «електронний (цифровий) доказ» у кримінальному процесі, установити критерії його допустимості й достовірності, процедури збирання, зберігання та використання таких доказів. Слід також розробити підзаконні акти чи стандарти, що деталізують технічні аспекти поводження з електронною інформацією (порядок створення копій, вилучення даних із хмарних сервісів, засвідчення їх автентичності тощо). Запровадження чітких правил усуне правову невизначеність і сприятиме однаковому застосуванню закону.

Подальший розвиток теорії та практики електронних доказів має відбуватися в тісному зв’язку з міжнародним досвідом. Деякі країни вже мають певні напрацювання щодо цифрових доказів –на рівні як права, так і технологій. Використання найкращих практик (наприклад, європейських підходів до транскордонного отримання електронних доказів, стандартів цифрової криміналістики тощо) допоможе Україні швидше розробити власну ефективну модель. У межах курсу на євроінтеграцію імплементація вимог і рекомендацій ЄС щодо електронних доказів видається необхідною та неминучою. Українська наукова спільнота вже започаткувала діалог у цьому напрямі, зосередивши увагу на браку узгоджених визначень та класифікацій і пропонуючи шляхи вирішення цього питання.

Отже, електронні докази становлять новий тип інформаційних носіїв, який потребує новітніх підходів у кримінальному судочинстві. Їх ефективне

використання дасть змогу підвищити якість доказування, передусім у справах про кіберзлочини й інших, де можуть бути традиційні речові докази. Для досягнення цієї мети науковці та законодавці мають спільно напрацювати універсальні рішення – від формулювання чіткого теоретичного поняття до детальної процедури фіксації та аналізу цифрових слідів. Тільки за умов належного теоретичного обґрунтування та законодавчого закріплення електронні докази цілком реалізують свій потенціал як повноцінний засіб встановлення істини в кримінальному провадженні, що відповідає викликам сучасного інформаційного суспільства.

1.2. Співвідношення понять «оригінал», «копія» електронних доказів

Електронний документ як джерело доказу, попри поширеність його застосування в доказуванні, ускладнює досягнення завдань кримінального провадження, що визначені в КПК України. Тому класифікація електронних документів за різноманітними чинниками має на меті вдосконаленню вимог перевірки й оцінки електронних документів, розроблення сучасної тактики та методики роботи з таким видом доказів. Важливими під час доказування є електронні докази, що обумовлено розвитком інноваційних технологій та застосуванням їх у різноманітних сферах суспільної діяльності. Також слід визначити співвідношення понять «оригінал» і «копія» електронних доказів. Електронні засоби використовують для вчинення кримінальних правопорушень чи приховування їх слідів, а також під час збирання та фіксації доказів учинення такого діяння чи обставин, які мають значення в кримінальному провадженні. Порядок застосування електронних доказів та їх статус у кримінальному процесуальному праві України мають бути чітко врегульованими в законодавстві. Проте необхідно зазначити про недостатність такого регулювання та наявність прогалин права стосовно питань, які стосуються електронних доказів у кримінальному процесі.

Питанням класифікації електронних документів й електронних доказів у кримінальному процесі досліджували А.-М. Ангеленюк [2], О. Гусєв [26], М. Гуцалюк [28], О. Козицька [47], В. Петрик [71], А. Ратнова [84], А. Скрипник [94], С. Хом'яченко [113] та ін. Проте, з огляду на динаміку розвитку інноваційних технологій, слід продовжувати детальне вивчення інституту електронних доказів у кримінальному процесі України.

О. Дегтярьова зазначає, що інформаційні технології зумовлюють постійну необхідність у передачі даних, обміном інформацією. Застосування електронних пристроїв у різних сферах життя є щоденною процедурою, однак і кількість правопорушень постійно збільшується. Оскільки дані знаходяться в електронній формі, механізм їх фіксації має певні процедурні особливості, зокрема закріплюючи їх як докази [29, с. 273].

Згідно зі ст. 84 КПК України, доказами в кримінальному провадженні є фактичні дані, одержані у визначеному законом порядку, на підставі яких слідчий, прокурор, слідчий суддя та суд встановлюють наявність чи відсутність фактів й обставин, що мають значення для кримінального провадження та підлягають доказуванню. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів [53].

Відповідно до ст. 98 КПК України, речовими доказами є матеріальні об'єкти, які були знаряддям здійснення кримінального правопорушення, зберегли на собі його сліди або мають інші відомості, які можуть бути застосовані як доказ факту чи обставин, що визначається під час кримінального провадження, зокрема предмети, які були об'єктом кримінально протиправних дій, гроші, цінності й інші речі, здобуті кримінально протиправним шляхом [53].

Згідно зі ст. 99 КПК України, документи є речовими доказами, якщо вони мають відомості, які можуть бути застосовані як доказ факту чи обставин, що встановлюють під час кримінального провадження. До документів можуть належати: матеріали фотозйомки, звукозапису, відеозапису й інші носії інформації (зокрема електронні), а також носії інформації, на яких за

допомогою технічних засобів зафіксовано процесуальні дії. У деяких випадках, а саме тоді, коли документ незмінний, він може мати водночас властивість і документа, і речового доказу [53].

Отже, електронні докази – це докази в кримінальних провадженнях, які можна одержати в електронній формі. Електронні докази одержують за допомогою електронних пристроїв, комп'ютерних носіїв інформації, а також комп'ютерних мереж, зокрема через мережу Інтернет. Вони стають доступними для сприйняття людиною після обробки засобами комп'ютерної техніки.

С. І. Хом'яченко й Т. О. Часова зауважують, що в кримінальному процесі електронний доказ – це інформація (відомості), що мають електронну (цифрову) форму про обставини, які підлягають обов'язковому доказуванню в кримінальному провадженні. До таких доказів потрібно віднести: текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі [113, с. 178].

Паралельно з терміном «електронні докази» (electronic evidence) часто використовують поняття «цифрові докази» (digital evidence), тому що на законодавчому рівні їх ще не визначено.

Інформацію, подану у формі, придатній для її оброблення електронними засобами, відповідно до Закону України «Про електронні документи та електронний документообіг», називають даними [81].

В Україні як юридичну категорію електронні докази започатковано 2017 року в ЦПК, ГПК і КАС України.

Відповідно до ст. 100 ЦПК України, ст. 96 ГПК України та ст. 99 КАС України, електронними доказами є інформація в електронній (цифровій) формі, що містить інформацію про обставини, які мають значення для справи, зокрема, електронні документи (текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних й інші дані в

електронній формі. Таку інформацію можуть зберігати, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (зокрема в мережі Інтернет). Триває робота щодо впровадження поняття «електронні (цифрові) докази» в законодавство України, зокрема в КПК України. Електронні дані, на противагу традиційним видам доказів, значно простіше змінити чи підробити, тому правоохоронцям необхідно дотримуватися таких правил поводження з даними, що дадуть змогу забезпечити допустимість доказів. На відміну від звичайних паперових документів, характеристики та просторові межі яких ми звикли бачити, електронні документи мають іншу природу та вирізняються такою характеристикою: електронний документ не може бути без носія інформації [11].

Значущими стають ідентифікаційні властивості носія інформації (зокрема найменування типу, марки моделі, індивідуального машинного носія, на якому записано документ); електронні докази не видимі для «неозброєного ока» (без спеціального інструментарію), для їх сприйняття та дослідження застосовують програмно-технічні засоби; вони можуть бути змінені, пошкоджені або знищені в процесі експлуатації пристрою користувачем чи під впливом фізичних чинників (високий рівень вологості, висока температура, електромагнітні випромінювання тощо); за стадіями виготовлення документи, зокрема електронні, поділяють на оригінали, дублікати, копії та виписки []. У ч. 3 ст. 99 КПК України зазначено, що оригіналом документа є власне документ, а оригіналом електронного документа – його відображення, якому надають таке само значення, як і документу. Проте для електронного документа такі поняття, як «оригінал», «дублікат», «копія», є умовними, тому що у усіх цих випадках електронний документ залишається оригіналом.

У ст. 7 Закону України «Про електронні документи та електронний документообіг» передбачено, що електронну копію та копію електронного документа на папері засвідчують у порядку, передбаченому законом, однак

відповідний нормативний акт досі не ухвалено [81]. Навіть нотаріуси не вповноважені державою засвідчувати такі копії.

У кримінальному процесі докази мають відповідати двом вимогам, які висувають до його змісту та форми, – належності (ст. 85 КПК України) і допустимості (ст. 86 КПК України). Відомо, що такі властивості повинен мати й електронний доказ, що можна забезпечити коректністю фіксації та подальшою незмінністю комп'ютерних даних.

В. В. Романюк та С. Є. Абламський вважають, що на нинішньому етапі розвитку суспільства вчинення кримінальних правопорушень супроводжується використанням цифрових (електронних) засобів, унаслідок чого, з одного боку, їх застосовують злочинці, а з іншого – слідчі для збирання доказів, які також мають цифрову (електронну) форму [85, с. 141].

Класифікація доказів – це поділ з метою дослідження складових цієї системи, яка має теоретичне та практичне значення для кримінального провадження. Завдяки такому поділу визначають особливості збирання, перевірки й оцінки доказів, їх важливість для доведення певних обставин, що стосуються предмета доказування. Таке різнопланове значення класифікації доказів засвідчує, що провести здійснити поділ доказів за однією ознакою неможливо.

Ми вважаємо, що електронний документ слід класифікувати за тими самими критеріями, які використовують для документів як джерел доказів. Водночас електронні документи, з огляду на їхні особливості, мають інші додаткові класифікаційні властивості.

На думку О. А. Самойленко, процеси глобальної цифровізації всіх сфер життя суспільства закономірно актуалізували проблеми застосування електронних (цифрових) документів як джерел доказової інформації в судочинстві різноманітних форм [87, с. 169]. За стадіями виготовлення електронні документи поділяють на оригінали, дублікати, копії та витяги.

У ч. 3, 4, ст. 99 КПК України визначено, що є оригіналом і дублікатом документа. Сторона кримінального провадження, потерпілий, представник

юридичної особи, стосовно якої здійснюють провадження, зобов'язані дати суду оригінал документа. Оригіналом документа є власне документ, а оригіналом електронного документа – його відображення, що має таке саме значення, як документ [53].

Дублікат документа (документ, зроблений таким самим способом, як і його оригінал), а також копії інформації, зокрема комп'ютерних даних, що містяться в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, суд визначає як оригінал документа [53].

Для підтвердження змісту документа можуть бути визнані допустимими й інші відомості, якщо: 1) оригінал документа втрачено або знищено, крім випадків, якщо його втрачено або знищено з вини потерпілого або сторони, яка його надає; 2) оригінал документа не може бути одержаний за допомогою доступних правових процедур; 3) оригінал документа знаходиться в користуванні однієї зі сторін кримінального провадження, а вона не надає його на запит іншої сторони. Сторона кримінального провадження, потерпілий, представник юридичної особи, стосовно якої здійснюють провадження, мають право надати витяги, компіляції, узагальнення документів, які незручно повністю досліджувати в суді, а на вимогу суду – зобов'язані надати документи в повному обсязі.

Сторона зобов'язана надати іншій стороні змогу побачити або скопіювати оригінали документів [53].

Отже, оригіналом електронного технічного документа є той, який створений та зберігається на первинному носії інформації. Наприклад, оригінал відеозапису з камер відеоспостереження зберігається на носії інформації, на який записують відео. Дублікатом (копією) такого відеозапису є його копіювання, переміщення, поширення на інший носії даних.

Ми вважаємо, що роздруківка вебсторінки, частини відео, фото чи іншого файлу не можуть бути визнані ні оригіналом, ні копією електронного документа, її самостійно не може бути використано як доказ. Візуалізована в паперовій формі сторінка може бути тільки додатком до проведеної слідчої (розшукової) дії. Належне виготовлення дубліката електронного документа забезпечує його допустимість під час перевірки доказів у суді.

Розглянемо приклад із судової практики. Зарічний районний суд м. Суми вироком від 28 квітня 2016 року за обвинуваченням в учиненні гр. П. кримінальних правопорушень, передбачених ч. 2 ст. 407, ч. 3 ст. 15, ч. 1 ст. 258-3 КК України, визнав роздруківки місця знаходження радіоелектронного засобу неналежними та недопустимими доказами. Відсутність первинних носіїв і зазначених відомостей у роздруківці та протоколі ставить під сумнів правдивість даних, що містяться в них, дає суду підстави стверджувати, що втручання в особисте спілкування гр. П. відбулося не в спосіб, що встановлений КПК України [12].

Також під час розгляду в судовому засіданні кримінального провадження стосовно обвинувачення гр. Ф. у вчиненні кримінального правопорушення, передбаченого ч. 1 ст. 258-3 КК України, Апеляційний суд м. Києва зазначив, що не можуть бути джерелом доказування та є недопустимими доказами фотокартки та скриншоти, одержані внаслідок моніторингу сторінок користувачів, яких орган досудового розслідування ототожнює з представниками ДНР, у соціальних мережах «Вконтакте» й «Одноклассники», тому що правдивість інформації, яка в них міститься, викликає обґрунтовані сумніви, їх одержано в спосіб, не передбачений кримінальним процесуальним законом [12]. Згідно з ч. 3, ч. 4, ст. 99 КПК України, сторона кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюють провадження, мають право представити витяги, компіляції, узагальнення документів, які незручно повністю досліджувати в суді, а на вимогу суду – зобов’язані представити документи в повному обсязі [108]. Витягом, компіляцією чи узагальненням

електронного документа є копіювання та виокремлення за допомогою технічних пристроїв частини інформації, яка встановлює наявність чи відсутність фактів й обставин, що мають значення для кримінального провадження та підлягають доказуванню. Витяг із документа – частина тексту документа. Витягом електронного документа є частина електронного документа. У витягу з електронного документа частина інформації та зміст ідентично відтворюються з базового документа [83; 84].

Обсяг і форма такого виокремлення даних чітко не встановлені, їх фактично визначають за внутрішнім переконанням слідчого та прокурора під час досудового розслідування. Основним завданням є відсіяти інформацію, що не є важливою, виявити інформацію, яка має значення під час доказування (вирізання частини звукозапису чи відеозапису, збільшення частини фотографії чи зображення, узагальнення змісту сторінки вебсайту тощо). Ця дія є суб'єктивною, тому оцінити правильність складання скороченого чи узагальненого електронного документа може тільки суд. Отже, якщо слідчий чи прокурор зробили витяг, компіляцію чи узагальнення електронного документа, то його разом із повним за обсягом і змістом оригіналом слід долучати до матеріалів кримінального провадження.

Одним із найскладніших є спосіб класифікації документів залежно від комбінацій метаданих – структурованих закодованих даних, які характеризують електронний документ і мають доказове значення в кримінальному провадженні [84]. Залежно від комбінації метаданих електронні документи можуть бути поділені на однорангові (наприклад, з розширенням *.wav, *.gif); дворангові; трирангові; чотирирангові, п'ятирангові (наприклад гіпертекст).

За доступом до даних метадані електронних документів можна поділити на відкриті та приховані. До відкритих метаданих належать ті, які звичайний користувач створює самостійно або може побачити за допомогою перевірки ознак документа. Наприклад, до них можна віднести дату й час створення, зміни, якщо це електронний лист, ім'я адресата, дату надсилання документа

тощо. Приховані метадані доступні користувачеві тільки через застосування спеціального технічного забезпечення та відповідних програм. Встановлення прихованих метаданих під час здійснення експертизи електронного документа надає можливість установити «електронні сліди» створення, редагування, видалення чи зміни документа.

Д. Ю. Рябущенко зазначає, що цифрові докази в кримінальному процесі є доволі дискусійною та складною категорією, по-перше, тому, що на нормативному вимірі не закріплено комплексної та вичерпної позиції законодавця з цієї проблематики; по-друге, через активну та неоднорідну дискусію на доктринальному рівні щодо перспективи інституціоналізації цифрових доказів у кримінальному процесі [86, с. 42].

За ступенем захисту електронні документи можна поділити на відкриті й закриті. Для захисту електронних документів є значна кількість спеціальних засобів: електронний цифровий підпис, шифрування поштових відправлень і мережевого трафіка, застосування систем захисту від несанкціонованого доступу в мережах, установка пароля на документі тощо [84].

За джерелом походження виокремлюють файли, які створюють користувач і комп’ютерна система (тобто електронне середовище). Автоматично створюються кеш-файли, cookie-файли, метадані за замовчуванням налаштувань програми тощо. Більшість електронних документів створює користувач, що передбачає введення даних особисто. Під час підключення до інтернету значна кількість даних про діяльність користувача зберігається в комп’ютері. Кеш-файли часто застосовують експерти під час вивчення електронних документів. Крім кеш-файлів, браузер також може зберігати cookie-файли, а саме дані про певного користувача в браузері та передачі на вебсайт, який раніше відвідували (наприклад, збереження пароля та логіна особистої сторінки, або ж вебсайт пропонує інформацію, послугу, товар, яким раніше цікавився користувач на іншому сайті). Аналіз судової практики засвідчує, що слідчі не часто, проте звертаються до суду для одержання інформації про дані з файлів cookie, що

зберігаються на пристрої, зокрема ідентифікатори та налаштування файлів cookie, файли cookie для користування поштовою скринькою тощо [84].

Класифікацію електронних документів можна здійснити за їх розміщенням: комп'ютер, смартфон, планшет, відеокамера, «розумна» побутова техніка, інтернет-сервер тощо. Дані про місцезнаходження електронного документа потрібні під час одержання санкціонованого доступу до нього та встановлення його особливостей, які виникають унаслідок існування на певному технічному носії інформації [84].

Доцільно зазначити, що електронні документи за формою можна поділити на відеозаписи, аудіозаписи, електронні повідомлення, вебсайти й інформацію в електронній формі. Під час аналізу судової практики встановлено, що часто суди досліджують такий вид електронного доказу, як відеозапис. Це можуть бути як відеозаписи з подією здійснення злочину, так і відеозаписи зі слідчими діями, слідчими експериментами тощо. Також є випадки вивчення судом аудіозапису (телефонних розмов з повідомленням про злочин, аудіозапис із плачем дитини та звуками ударів тощо). Крім того, трапляються випадки дослідження скриншотів електронних сторінок з листуванням.

Розглянемо проблемні питання використання електронних доказів у кримінальному процесуальному праві України, серед яких:

1. Невідмежованість електронного доказу від інших джерел доказів. У науці не сформовано єдиного розуміння місця електронних доказів у системі процесуальних джерел доказів: наявні аргументи на користь як віднесення їх до традиційних (речові докази, документи), так і виокремлення їх у самостійну групу (цифрові чи електронні докази). У судовій практиці є випадки визнання судом електронними доказами файлів, а речовими доказами – носіїв, на яких вони знаходяться. В інших випадках суд розглядає електронні докази як електронні документи [94, с. 96]. Необхідно зауважити, що поняття електронного документа є вужчим, порівняно з розумінням електронного доказу. Зокрема, електронний документ має містити обов'язкові реквізити, які

властиві документам. Своєю чергою електронний доказ не завжди має такі реквізити, проте має відомості, які є доказовим фактом. З огляду на правову природу електронного доказу, у науці аргументовано виокремлення носіїв електронної інформації в самостійне процесуальне джерело доказів, тож вважаємо це слушним.

Поняття речового доказу, електронного документа й електронного доказу не тотожні, а зазначена вище оцінка суду обумовлена прогалинами права стосовно визначення електронних доказів та їх статусу в кримінальному процесі України.

Згідно з ч. 2 ст. 84 КПК України, процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів [53]. Отже, електронні докази залишилися поза увагою.

2. Невизначеність джерел одержання електронних доказів у кримінальному провадженні. Джерела одержання електронних доказів у кримінальному провадженні не визначено в положеннях КПК (аналогічно з поняттям електронних доказів під час доказування кримінального правопорушення). Певне розуміння джерел одержання електронних доказів у кримінальному процесі формує практика, зокрема судова, де суд дає оцінку електронним доказам за ознакою допустимості:

– запис телефонної розмови є допустимим доказом за умови, що на телефоні працює програма автоматичного запису всіх розмов його власника;

– розмова, зафіксована потерпілим на диктофон, є недопустимим доказом, якщо запис було здійснено цілеспрямовано;

– відеозаписи створено за допомогою системи відеоспостереження міста Києва є допустимими доказами й не мають ознак проведення НСРД, тому що фіксація за допомогою цієї системи є відкритою та спрямована на спостереження за визначеними об’єктами.

Необхідно зауважити, що суд у частині випадків зобов’язаний вивчати прогалини права. З метою оптимізації часу, витраченого на кримінальне провадження, потрібно усувати ці прогалини в законодавстві. Зокрема, у

кримінальному процесуальному законодавстві було б доцільним окремою статтею визначити джерела одержання електронних доказів у кримінальному провадженні та внести відповідні доповнення в КПК.

3. Недостатність нормативно-правового регулювання щодо застосування копії електронних доказів, оригінали яких утрачено. Згідно з ч. 4 ст. 99 КПК, копії інформації, зокрема комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, суд визнає оригіналом документа. Крім того, ч. 5 ст. 99 КПК України визначає випадки, коли для підтвердження змісту документа можуть бути визнані допустимими й інші відомості, а саме в разі втрати або знищення документа або неможливості його одержання.

Проте під час практичної діяльності можуть траплятися ситуації, де практична реалізація вимог КПК України значно ускладнюється. Наприклад, відеозапис камери відеоспостереження скопіював на флешносій власник, тому що записи мають нетривалий термін зберігання (накладають наступний запис на попередній), тому оригінал запису зберегти не вдалося. Копія електронного доказу не може бути допустимим доказом факту чи обставин, на доведення яких її надано, якщо відомості, які вона має, не підтверджують іншими доказами, визнаними допустимим.

4. Обмеження можливостей дізнавача стосовно застосування електронних доказів. З огляду на інститут дізнання в кримінальному процесуальному праві, який нещодавно запроваджено, слід зауважити, що дізнавач під час розслідування повинен мати законні підстави застосовувати ресурси, які надаватиме інформаційно-телекомунікаційна система досудового розслідування, що безпосередньо пов'язано з процесом збирання та вивчення електронних доказів.

5. Неорганізованість роботи інформаційно-телекомунікаційної системи досудового розслідування за участю Національної поліції України. Згідно зі

ст. 106-1 КПК слідчий, дізнавач, прокурор, слідчий суддя, суд, а також захисник (за його згодою) застосовують, а інші учасники кримінального провадження можуть застосовувати інформаційно-телекомунікаційну систему досудового розслідування під час реалізації своїх повноважень, прав й інтересів, передбачених КПК, за умов і в порядку, що визначені положенням про таку систему.

Своєю чергою порядок функціонування інформаційно-телекомунікаційної системи досудового розслідування визначають положенням, яке затверджують спільно Офіс Генерального прокурора, орган, у складі якого функціонує орган досудового розслідування, а також орган, що затверджує положення про систему, яка функціонує в суді згідно зі ст. 35 КПК [2, с. 215–217].

Використання електронних доказів у кримінальному процесі стає актуальнішим, що зумовлено розширенням масштабів застосування інноваційних цифрових технологій у суспільстві загалом. Тож необхідною є чітка регламентація в законодавстві питань, пов’язаних із застосуванням електронних доказів під час досудового розслідування в кримінальному провадженні. Електронні докази мають бути визнані окремим джерелом доказів. У нормах КПК слід визначити перелік можливих джерел одержання електронних доказів, які згодом стануть частиною кримінального провадження. Потребує доопрацювання питання застосування в кримінальному провадженні електронних копій доказів, оригінали яких втрачено [2]. У зв’язку з проведенням у частині випадків досудового розслідування у формі дізнання, доцільно закріпити в законодавстві положення щодо роботи з електронними доказами дізнавачів як суб’єктів сторони обвинувачення в кримінальному процесі. У застосуванні інформаційно-телекомунікаційної системи досудового розслідування слід ураховувати особливості електронної форми доказів з метою забезпечення їх допустимості у суді [59].

1.3. Міжнародно-правовий досвід використання електронних доказів як засобу доказування в кримінальному провадженні

Стрімкий розвиток цифрових технологій та поширення кіберзлочинності зумовили появу нового виду доказів – електронних (цифрових) доказів, які набувають ключового значення в кримінальному судочинстві. Правоохоронні органи в усьому світі усвідомлюють необхідність ефективної роботи з електронними даними, що мають доказове значення, однак законодавство деяких країн відстає від темпів технологічного прогресу. В Україні лише нещодавно реалізовано кроки до нормативного закріплення цього поняття: 2017 року поняття «електронні докази» було введено до процесуальних кодексів (цивільного, господарського, адміністративного), а Законом від 15 березня 2022 року № 2137-IX удосконалено регулювання збору й використання електронних доказів у кримінальному провадженні. Водночас залишаються невирішеними питання щодо чіткого визначення електронних доказів, правил їх збирання та перевірки, а також належної процедури міжнародного обміну такими даними. Актуальність дослідження зумовлена необхідністю розроблення єдиних підходів до поводження з електронними доказами та врахування міжнародно-правового досвіду їх використання для підвищення ефективності та законності доказування в кримінальному процесі.

Науковці та практики по-різному визначають сутність електронних доказів, що відображає новизну цього поняття та брак усталеної термінології. В англомовній літературі поширені терміни «electronic evidence» («електронний доказ») і «digital evidence» («цифровий доказ»), які здебільшого вважають синонімами [88]. В українській правничій думці також немає єдиного підходу: одні автори пропонують використовувати термін «електронні докази» як загальноприйнятий у кримінальному процесі. На думку Н. М. Ахтирської, поняття електронних доказів охоплює будь-які дані, які підтверджують факти чи обставини та представлені у формі, придатній для обробки комп’ютерними системами [5]. В. В. Мурадов визначає електронні

докази як сукупність інформації, що зберігається в електронному вигляді на різноманітних носіях [64]. І. О. Крицька вводить поняття «цифрові джерела доказової інформації», до яких відносить програми, файли баз даних, аудіо- та відеозаписи, що зберігаються на пристроях для накопичення даних (жорстких дисках, оптичних і флешнакопичувачах тощо) [54]. Отже, попри різні формулювання, спільним є розуміння електронного доказу як інформації в цифровій формі, що має значення для кримінального провадження.

Слід зазначити, що в законодавствах різних держав досі немає легального визначення електронних доказів, і це підтверджує міжнародний досвід. У національному законодавстві Австрії, Болгарії, Чехії, Італії, Швеції та інших країн немає офіційного визначення терміна «електронні докази» [88]. Натомість використовують доктринальні підходи або загальні положення доказового права. У Португалії науковці визначають електронний доказ як будь-яку інформацію, що має доказове значення та зберігається або передається в цифровій (двійковій) формі. У Німеччині електронними доказами вважають інформацію, збережену чи передану в цифровому форматі, яка суттєва для розслідування злочину. Французький підхід охоплює будь-яку доказову інформацію, створену, збережену або передану в електронній формі за допомогою цифрових пристроїв, що є важливою для досудового слідства. Прикметно, що у Франції приклади електронних доказів безпосередньо охоплюють електронні листи, текстові повідомлення, фотографії, відео з інтернету, а також дані абонентів і трафік онлайн-акаунтів [88]. У всіх цих випадках законодавець фактично прирівнює електронні (цифрові) докази до традиційних, надаючи їм таку саму юридичну силу, як паперовим носіям інформації. Аналіз засвідчує, що більшість розвинених країн адаптували норми доказування, розроблені ще для матеріальних доказів, до нових цифрових реалій, замінюючи паперові документи їх електронними аналогами. Спеціальних окремих процедур чи кодексів саме для роботи з електронними доказами ніде не передбачено: електронні документи інтегровано в загальну систему доказів, найчастіше як різновид письмових доказів [88].

В. М. Стратонов акцентує на тому, що в сучасних умовах збройних конфліктів питання документування порушень міжнародного гуманітарного права, зокрема фактів експлуатації людини, набуло важливого значення в контексті забезпечення ефективного міжнародного кримінального правосуддя. Новизна теми полягає в системному аналізі інтеграції технологічних інструментів, таких як OSINT (відкриті джерела розвідки), супутниковий моніторинг, цифрова верифікація доказів, штучний інтелект, у механізми виявлення, фіксації та процесуального доведення випадків примусової праці, сексуального рабства, залучення дітей до воєнних дій тощо. З огляду на транснаціональний характер таких порушень, застосування технологій є необхідною умовою формування достовірної та прийнятної доказової бази у справах, що розглядають Міжнародний кримінальний суд, спеціалізовані трибунали чи регіональні суди [103].

У світовій спільноті досі немає уніфікованого міжнародного чи європейського визначення електронних доказів і єдиної правової бази щодо їх поводження. Кожна держава керується переважно власним законодавством у питаннях збирання, зберігання, перевірки й обміну цифровими доказами. Традиційні кримінально-процесуальні норми більшості країн було прийнято ще до епохи інтернету, тому деякі держави внесли зміни для врахування електронної форми доказів, а інші продовжують застосовувати старі норми, просто екстраполюючи їх на нові цифрові об’єкти. Така ситуація призводить до розбіжностей у термінології та процедурах, що ускладнює взаємне визнання та обмін доказами між різними країнами. Згідно з дослідженням ООН, навіть держави зі схожими правовими традиціями часто мають суттєві відмінності в правилах поводження з доказами, що створює перешкоди для міжнародного співробітництва в боротьбі зі злочинністю в кіберпросторі [146].

Міжнародна практика демонструє визнання допустимості цифрових матеріалів, отриманих з відкритих джерел, включно з відеозаписами, метаданими, координатами тощо, за умови забезпечення ланцюга збереження

(chain of custody), технічної верифікації та експертної оцінки. Аналогічно докази, отримані з OSINT-джерел або мобільних пристроїв, визнає МКС у справах про залучення дітей до бойових дій, трудову експлуатацію або примусову депортацію. Отже, першим кроком у напрямі гармонізації українського кримінального процесуального законодавства з міжнародними стандартами є закріплення на рівні КПК: поняття «цифровий доказ» з переліком джерел (OSINT, відео, супутникові знімки, соціальні мережі); стандарти автентичності, релевантності, цілісності, верифікованості та законності походження; обов'язкову участь технічного експерта для аналізу цифрових матеріалів і метаданих; право сторін процесу оскаржувати спосіб отримання цифрових доказів [103].

Утім міжнародні організації напрацьовують рекомендації щодо цифрових доказів. Важливим кроком стало прийняття 2001 року Будапештської конвенції про кіберзлочинність, яка запровадила механізми спрощеної взаємодії між державами в зборі електронних доказів (наприклад, оперативне збереження даних, транскордонний доступ до відкритих даних) і встановила стандарти поводження з комп'ютерною інформацією. Попри це, практична реалізація міжнародних запитів про правову допомогу (MLAT) у цій сфері залишалася тривалою та складною процедурою: для отримання електронних доказів, що зберігаються на серверах за кордоном, необхідно було надсилати офіційні запити до компетентних органів іншої країни, очікування відповідей могло тривати місяцями [159]. Лише незначна кількість держав мала спрощені механізми доступу до закордонних даних на двосторонньому рівні [159]. Така ситуація стимулювала появу нових міжнародно-правових інструментів. Зокрема, зусиллями Ради Європи було розроблено Другий додатковий протокол до Конвенції про кіберзлочинність (2022), який передбачає прямий доступ правоохоронців до певних електронних даних від закордонних провайдерів й інші сучасні способи співпраці. Сполучені Штати Америки ухвалили закон CLOUD Act (2018), що дозволяє укладати угоди з іноземними державами для прямих запитів до

провайдерів стосовно даних користувачів, розміщених на серверах у США, оминаючи звичайну процедуру MLAT. Ці кроки засвідчують глобальну тенденцію до спрощення доступу слідчих органів до інформації в електронному вигляді, яка часто фізично знаходиться за межами їхньої юрисдикції.

Н. М. Ахтирська й О. Ю. Костюченко вважають, що міжнародне співробітництво під час кримінального провадження та особливості збору електронних доказів, які знаходяться під управлінням закордонного постачальника послуг, є ще одним актуальним питанням за цим напрямом. Кримінальний процесуальний кодекс України не містить визначення електронних доказів, проте кримінальне судочинство дедалі частіше постають перед необхідністю збору, оцінки та використання таких доказів для ухвалення вироків. Відсутність нормативної визначеності не сприяє єдності судової практики, гостро постає питання щодо оцінки електронних доказів, одержаних у межах міжнародної правової допомоги. У таких ситуаціях доводиться оцінювати правомірність діяльності правоохоронного органу, дотримання конвенційних гарантій дотримання прав людини, виконання зобов’язань використовувати електронні докази виключно в тому провадженні, на запит у якому вони були одержані, перевіряти факт повторного звернення до центрального органу міжнародного співробітництва в іншій державі з клопотанням про надання дозволу про використання таких доказів в іншому провадженні, коли постала така потреба тощо. Суди розглядають клопотання прокурора про тимчасовий доступ до електронних даних або про проведення обшуку, інколи припускаються помилки, вказуючи юрисдикцію, де виникли докази, або де наступили наслідки злочинної діяльності. Процесуальні вимоги, які передбачені міжнародними актами, зумовлюють потребу звернення до держави, на території якої перебуває суб’єкт, який володіє, накопичує та здійснює управління даними [7].

На рівні ЄС протягом тривалого часу також нагальною була потреба в єдиному підході до електронних доказів. Хоча національні законодавства

країн – членів ЄС здебільшого визнають електронні документи рівноцінними паперовим [138], брак спільного правового механізму ускладнював транскордонні розслідування. Згідно зі статистичними даними, понад 50 % усіх кримінальних розслідувань у Євросоюзі потребують отримання електронної інформації з іншої країни [159]. Дотепер процес отримання таких даних із-за кордону був громіздким: потрібно було використовувати процедури міжнародної допомоги, чекати виконання запитів тощо [159]. Для розв'язання цієї проблеми Європейська комісія ініціювала «пакет електронних доказів» (e-evidence package). У липні 2023 року ЄС ухвалив два ключові акти: Регламент (ЄС) 2023/1543 про Європейські ордери на пред'явлення та збереження електронних доказів у кримінальному провадженні [149] та Директиву (ЄС) 2023/1544, що встановлює гармонізовані правила визначення представництв постачальників послуг для вручення таких ордерів [132]. Нові акти набувають чинності 2026 року та зобов'язують кожну державу-члена призначити в межах ЄС уповноваженого представника (або установу) для отримання вимог про надання даних [159]. Головне нововведення – можливість для судових органів однієї країни прямо звертатися з європейським ордером до інтернет-сервіс провайдера, який діє на території іншої країни, без необхідності проходження традиційного міждержавного запиту [159]. Наприклад, прокурор у Франції зможе направити провайдеру електронної пошти в Німеччині ордер на видачу електронних листів підозрюваного, і провайдер буде зобов'язаний надати запитані дані протягом встановленого строку (до 10 днів, а в термінових випадках – до 8 год) [159]. Регламент 2023/1543 також чітко визначає категорії даних, які можуть запитувати: це дані абонента (ідентифікаційна інформація користувача), дані трафіка (лог-файли, маршрути передачі) і контент (зміст повідомлень, файлів тощо) [149]. Встановлено гарантії захисту прав: для отримання контенту і трафіка є вимога щодо повідомлення держави-виконавця ордера, яка може відмовити у виконанні за певних обставин (наприклад, якщо це загрожує національним інтересам або суперечить основним правам) [159]. Отже, ЄС

реалізує важливий крок до спрощення та уніфікації доступу до електронних доказів у межах Союзу, скорочуючи залежність від повільних процедур взаємної правової допомоги.

Водночас впровадження нових правил потребуватиме високого рівня взаємної довіри між державами-членами та належного врахування національних правових особливостей [88]. Попри загальний регламентований порядок, деякі питання (наприклад, допустимість отриманих даних у суді) все одно вирішуватимуть у межах національного права держави, що розглядає справу. Тому гармонізація не скасовує необхідності вдосконалення внутрішніх процедур роботи з електронними доказами.

Прикладом регіонального акта, присвяченого правовому регулюванню використання доказів в електронній формі, є Проєкт модельного закону Співдружності держав Карибського басейну про електронні докази 2017 року (Commonwealth Draft Model Law on Electronic Evidence). Серед основних положень цього документа доцільно зазначити такі. На електронні докази поширюються властивості належності, допустимості й достовірності, за винятком випадків, визначених цим актом. Доказ не може бути визнано недопустимим лише на тій підставі, що він має електронну форму. З метою перевірки допустимості електронних даних можуть бути подані докази щодо будь-якого стандарту або практики того, як ці електронні дані повинні бути записані або збережені, з огляду на тип діяльності, у межах якої їх використовували, а також характер і мету електронних даних. Сторона, яка подає електронний доказ, несе тягар доказування його достовірності. Якщо немає доказів протилежного, цілісність електронних даних або системи, у якій записано чи зберігаються такі дані, презюмується в будь-якому судовому процесі: а) за наявності доказів, які підтверджують висновок про те, що в усі істотні моменти часу комп’ютерна система або аналогічний пристрій працював належно, або, якщо це не так, то такі обставини не вплинули на цілісність даних, а також немає інших розумних сумнівів щодо їх цілісності; б) якщо буде встановлено, що електронні дані були записані або зберігалися

стороною, інтереси якої не відповідають інтересам сторони, яка прагне їх подати; в) якщо встановлено, що електронні дані були записані або зберігалися у звичайному процесі ведення діяльності особою, яка не є стороною провадження, яка не записувала провадження та не здійснювала запис або зберігання під контролем сторони, яка бажає подати ці дані. З метою перевірки допустимості й достовірності електронних даних особа, яка їх подала, може бути піддана перехресному допиту стороною з протилежними інтересами. Якщо інше не передбачене будь-яким іншим законом, електронні дані можуть бути визнані допустимими на розсуд суду, якщо сторони судового провадження прямо погодилися, що їх допустимість не може бути оспорена. Угода між сторонами щодо допустимості електронних даних не робить їх допустимими в кримінальному провадженні, якщо на момент укладення цієї угоди обвинувачений не мав захисника [111; 129].

Розглянемо також досвід США та Великої Британії. У правових системах країн загального права значним є практичний досвід поводження із цифровими доказами, що ґрунтується на прецедентах і поступовому пристосуванні норм доказування до технічних новацій. У США основні вимоги до доказів визначено у Федеральних правилах доказів 1975 року. Зокрема, правило 401 встановлює широке визначення релевантності: доказ вважають допустимим, якщо він здатен вплинути на ймовірність існування факту, що має значення для справи [88]. Електронні документи за природою не відрізняються від інших доказів з погляду релевантності, проте виникають додаткові питання автентичності й надійності цифрових даних. Перед прийняттям електронного доказу суди США вимагають продемонструвати його автентичність: сторона, яка подає доказ, повинна довести, що цей електронний документ є справжнім і саме тим, за що себе видає. Для цього використовують процедуру, передбачену правилом 901 (наприклад, свідчення особи, що створила документ, або технічна експертиза). Також у судовій практиці напрацьовано стандарти щодо ланцюжка збереження (chain of custody) цифрових доказів, аби унеможливити їх підроблення чи зміну під час

слідства. Відомі прецеденти, як-от Lorraine v. Markel (2007) [135], детально описують критерії допустимості електронних листів, чат-повідомлень, даних з інтернету тощо: суди перевіряють не лише релевантність, а й те, чи були дані отримані законно, чи збережено їх цілісність, чи відповідають вони правилам hearsay (похідних доказів) тощо. Отже, американський досвід демонструє, що на основі гнучких загальних правил доказування можливо пристосувати судову процедуру до будь-яких нових видів доказів, розробивши практичні тести і критерії для їх оцінювання.

З огляду на збільшення кількості випадків використання інформаційно-комунікаційних технологій зі злочинною метою, а також потерпілих від кіберзлочинів, важливість забезпечення правосуддя для захисту прав потерпілих та обов'язку держави нести відповідальність за захист суспільства не тільки в реальному світі, а й в інтернеті, зокрема шляхом ефективного використання електронних доказів, які знаходяться під юрисдикцією іноземних держав, доцільно: на законодавчому рівні (шляхом прийняття спеціального закону «Про електронні докази») визначити поняття електронних доказів, види, способи збирання, оцінки та використання; встановити процесуальні строки звернення з клопотанням про зберігання електронних доказів (первинне та повторне) з огляду на законодавство США, оскільки великі постачальники послуг перебувають під їх юрисдикцією; вказати на необхідність перевірки судами мети первинного звернення за одержанням доказів і кримінального провадження, оскільки використання електронних доказів в іншому кримінальному провадженні може призвести до визнання таких доказів неприйнятними [7].

Право Великої Британії також визнало електронні докази задовго до появи спеціальних норм ЄС. Ще Закон про поліцію та докази в кримінальних справах 1984 року (PACE) надав повноваження слідчим вилучати «будь-які документи, зокрема електронні записи» під час обшуків, якщо вони можуть містити доказову інформацію. Отже, уже базове визначення поняття *document* у британському праві охоплює електронні дані, що підтверджують факти.

Згодом британські суди розробили підходи до оцінки автентичності цифрових доказів на основі принципу «найкращого доказу» (best evidence rule): за можливості треба надавати оригінальний електронний носій або його достовірну копію, а не роздруківку. Хоча специфічного закону про електронні докази в кримінальному процесі в Британії немає, є детальні керівництва для слідчих й експертів (наприклад, ACPO Good Practice Guide for Digital Evidence), які стандартизують процес збирання та аналізу цифрової інформації, щоб забезпечити її допустимість у суді. Ці керівні документи акцентують на важливості дотримання принципу незмінності даних (жодного редагування оригіналу), документування всіх дій з електронним носієм і використання належних методів цифрової криміналістики. Британський досвід цікавий також активним упровадженням технологій штучного інтелекту в роботу з електронними доказами, наприклад, для швидкої перевірки великих обсягів даних чи прогнозування релевантності інформації, яку розглядають у справі [123].

Комітет безпеки Європейського Союзу визначає електронні докази як дані, що зберігають в електронному вигляді, наприклад, IP-адреси, електронні листи, фотографії або імена користувачів, які мають значення для кримінального процесу. Такі дані знаходяться в постачальників послуг, а правоохоронні та судові органи змушені звертатися до них для отримання необхідної інформації. У національному законодавстві Австрії, Болгарії, Чехії, Італії, Швеції та інших держав офіційного визначення електронних доказів немає. Законодавство Португалії також не містить визначення терміна «електронний доказ», однак у цій країні використовують 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 [43; 83, с. 169].

Китайська Народна Республіка є прикладом країни, яка в стислий проміжок часу імплементувала електронні докази у свою систему права, урахувавши національні особливості. 2012 року до КПК КНР було внесено

зміни, якими електронні докази формально прирівняли до традиційних засобів доказування [88]. Хоча визначення цього поняття в законі спершу не було, згодом Верховний народний суд Китаю видав спеціальне роз'яснення «Про деякі питання збирання, отримання та аналізу електронних даних у кримінальних справах» (2016), де наведено перелік того, що охоплено поняттям електронних доказів. Зокрема, до електронних доказів віднесено інформацію з вебсайтів, блогів, соціальних мереж, онлайн-форумів і хмарних сховищ; електронні листи, мобільні повідомлення, чати в месенджерах і групах; дані електронних транзакцій і лог-файли систем; дані реєстрації користувачів тощо [88]. Отримання таких доказів дозволено лише для уповноважених слідчих у присутності не менше ніж двох понятих, із дотриманням встановлених процесуальних вимог і технічних стандартів, щоб гарантувати автентичність та цілісність даних. Отже, китайський підхід схожий на європейський у тому, що електронним доказам надано формальний статус, але для їх використання встановлено суворі процедури, з огляду на масштаб країни та величезні обсяги цифрових даних. Окрім Китаю, слід зазначити про досвід інших азійських держав: наприклад, Сінгапур увів правила щодо комп'ютерних доказів ще у 1990-х роках, Індія внесла поправки до Закону про докази (Indian Evidence Act) у 2000 році, додавши положення про електронні записи та їхню презумпцію достовірності за певних умов. Низка країн Близького Сходу та Латинської Америки нині переймають положення моделі закону ЮНСІТРАЛ про електронну комерцію щодо надання електронним документам юридичної сили, застосовуючи їх і в кримінальному судочинстві.

Європейський суд з прав людини (ЄСПЛ) розглядає питання цифрового нагляду та збирання електронних доказів крізь призму ст. 8 Європейської конвенції про права людини, яка гарантує право на повагу до приватного і сімейного життя, дому та кореспонденції [48]. Суд трактує поняття «приватне життя» широко: у сферу захисту потрапляють не лише особисті відносини, а й різноманітні аспекти цифрових комунікацій. Зокрема, у справі Copland v.

United Kingdom Суд встановив, що телефонні дзвінки, електронні листи та користування інтернетом на робочому місці за відсутності чіткого повідомлення про моніторинг мають «природний статус приватного життя та кореспонденції» [130]. Аналогічно ЄСПЛ визнав, що навіть мобільні дзвінки включають до поняття «приватного життя» [130]. Водночас Суд зауважує, що працівник може мати виправдані очікування конфіденційності своїх електронних повідомлень, якщо йому не роз'яснено порядок та обсяг контролю [139]. У справі Bărbulescu v. Romania Суд зазначив, що хоча моніторинг повідомлень може бути виправданим, держави повинні забезпечити «адекватні й достатні» гарантії від зловживань. Отже, ЄСПЛ зберігає баланс: він допускає нагляд за приватними комунікаціями лише з огляду на права особи на захист приватності.

Важливою вимогою ст. 8 є «відповідність втручання законові». Суд неодноразово акцентував, що будь-яка форма цифрового нагляду повинна мати чітке законодавче підґрунтя та відповідати критеріям передбачуваності. У справі Copland v. United Kingdom ЄСПЛ установив, що моніторинг працівника без жодного нормативного акта чи внутрішньої політики не відповідав «вимозі передбаченості закону» [130] і порушував ст. 8. У справі Roman Zakharov v. Russia Суд детально розглянув російські норми про перехоплення мобільних дзвінків і дійшов висновку, що вони не забезпечують достатньої ясності та гарантій. Відсутність чіткого визначення обсягу повноважень органів, можливості обходу судового контролю та наявного засобу захисту для особи означає, що «закон» не відповідає критеріям якості й передбачуваності [158]. Тож у випадках, коли нормативна база нагляду була нечіткою або її взагалі не було, ЄСПЛ визнавав втручання в особисте життя незаконним, як-от у справі Copland v. United Kingdom і Roman Zakharov v. Russia.

Одночасно ЄСПЛ вимагає, щоб втручання було необхідним у демократичному суспільстві та пропорційним поставленій меті. Успадкованим підходом є принцип, викладений у справі Klass and Others

v. Germany (1978): секретні заходи спостереження можуть бути виправданими лише за крайньої необхідності задля національної безпеки або запобігання тяжким злочинам [136]. Загальною практикою ЄСПЛ є суворо зіставляти масштаби нагляду з реальною загрозою. У справі Roman Zakharov v. Russia Суд зауважив, що масове прослуховування без адекватних обмежень і процесуальних гарантій не відповідало жодній вагомій меті та було непропорційним [158]. Натомість у справі Uzun v. Germany GPS нагляд за пересуванням підозрюваного-терориста був визнаний виправданим: його здійснювали на основі чітко визначеного кримінально-процесуального закону протягом обмеженого проміжку часу (завершився після тримісячного спостереження) і лише після того, як менш інвазивні методи (візуальне спостереження, приховані передавачі тощо) виявилися неефективними [136]. Суд констатував, що такий нагляд мав законну мету («охорона національної безпеки, запобігання злочинам, захист прав жертв») і був пропорційним обставинам (серйозність злочинів й обмежений характер спостереження) [136]. Отже, ЄСПЛ допускає використання електронних доказів у кримінальних розслідуваннях за умови дотримання вимог законності, необхідності та пропорційності.

Суд також виокремив низку факторів для оцінки пропорційності моніторингу в робочому контексті. Зокрема, за рішенням Гранд-палати ЄСПЛ у справі Bărbulescu v. Romania національні органи повинні з’ясувати:

– попереднє повідомлення працівника та характер нагляду. Працівник має бути поінформований про можливість моніторингу та його сутність (які саме комунікації контролюватимуть). У повідомленні мають бути чітко визначені спосіб та обсяг контролю (зокрема, він стосується лише метаданих чи й вмісту листування);

– ступінь масштабності й інвазивності нагляду. Встановлюють, чи йшлося лише про перевірку фактів (потоку інформації) чи про зчитування змісту повідомлень. Оцінюють, чи моніторили всі комунікації чи частково, протягом якого проміжку часу і за участю скількох осіб [157];

– вагомість причин й обґрунтованість методів. Оцінюють, чи обґрунтовані підстави для моніторингу (наприклад, можливе зловживання робочим часом) і чи можна було обмежитися менш інвазивними засобами (наприклад, контролювати лише лог-записи, а не вміст) [157]. Наслідки та використання результатів. Аналізують, як отримана інформація вплинула на працівника та чи використовували її відповідно до заявленої мети. Зокрема, увагу зосереджено на питанні: чи було використано результати моніторингу саме для захисту інтересів роботодавця, заявлених у правилах внутрішнього розпорядку [157]; наявності гарантій проти зловживання. Наприклад, якщо контроль поширюється на вміст листування, повинні бути запроваджені механізми, що не дозволяють роботодавцю самостійно читати повідомлення, якщо працівника про це не попередили заздалегідь [157].

Отже, у рішеннях ЄСПЛ прослідковується чітка установка: держава-партнер має створити і підтримувати законодавчі та процесуальні механізми, які надавали б можливість органам влади чи роботодавцям здійснювати цифровий нагляд виключно у випадках гострої необхідності та з дотриманням прав людини. Відсутність таких гарантій є підставою для визнання втручання не сумісним із конвенційними стандартами. Тож ЄСПЛ у низці рішень встановив порушення ст. 8, зокрема у справах Copland v. United Kingdom (моніторинг без правової основи) [130], Bărbulescu v. Romania (недостатнє інформування про обсяг нагляду) [139] та Roman Zakharov v. Russia (законодавство про секретний нагляд) [158]. Натомість, коли втручання задовольняє вимоги правомірності та пропорційності, ЄСПЛ не знаходить порушень (як у Uzun v. Germany, де GPS-нагляд був санкціонований законом і тривав обмежений проміжок часу за умов особливої вагомості злочину [136]).

Отже, здійснений аналіз засвідчив, що електронні докази стали невіддільним елементом сучасного кримінального правосуддя, передусім у контексті боротьби з кіберзлочинністю і транскордонною злочинністю. Попри відсутність єдиного загальновизнаного визначення цього поняття на міжнародному чи навіть європейському рівнях, більшість країн фактично

визнають електронні докази рівнозначними традиційним (паперовим) і поступово адаптують свої правові норми до умов цифрового середовища. Водночас зберігаються значні розбіжності в термінології, підходах до збирання, зберігання та обміну електронною інформацією, що ускладнює взаємодію правоохоронних органів різних держав. Ініціативи Європейського Союзу, такі як Регламент 2023/1543 і Директива 2023/1544, мають частково усунути ці проблеми шляхом гармонізації процедур доступу до цифрових доказів. Проте ефективність цих нововведень залежатиме від готовності держав до співпраці та взаємної довіри, а також від урахування національних правових особливостей під час імплементації єдиних правил. Важливо, щоб спрощення отримання електронних доказів не порушувало баланс між інтересами правосуддя та фундаментальними правами людини: потреба дотримання права на приватність під час збору цифрових даних підтверджена практикою ЄСПЛ.

Для України результати цього дослідження мають практичне значення в контексті наближення до європейських стандартів. Урахування найкращих міжнародних практик у сфері електронних доказів сприятиме вдосконаленню національного законодавства та правозастосування. На шляху євроінтеграції Україна вже реалізувала перші кроки, визнавши електронні докази процесуальним засобом доказування, проте необхідно продовжити роботу в напрямі деталізації процедур їх вилучення, перевірки й оцінки. Запозичення досвіду ЄС (зокрема імплементація положень нещодавніх регламентів ЄС) допоможе забезпечити ефективну взаємодію з правоохоронними органами держав-членів у справах, що вимагають транскордонного отримання даних. Водночас слід посилити гарантії захисту прав людини в роботі з електронними доказами, аби нові інструменти розслідування не порушували зобов’язань України за міжнародними конвенціями. Отже, міжнародно-правовий досвід використання електронних доказів дає цінний матеріал для розвитку національної доктрини та практики доказування в цифрову епоху, забезпечуючи баланс між ефективністю правосуддя і правами особи.

Висновки до розділу 1

1. З’ясовано, що в доктрині кримінального процесу електроні докази тлумачать як: носії інформації, що потребує спеціальних процедур фіксації, збереження та перевірки достовірності (О. Капліна, М. Шумило, Р. Юрка); фактичні дані, що зберігають в електронному вигляді на будь-яких видах носіїв і стають доступними для сприйняття людиною після обробки спеціальними технічними засобами й програмним забезпеченням (Д. Алєксєєва-Процюк, О. Брисковська); інформацію (відомості), що мають електронну (цифрову) форму про обставини, які підлягають обов’язковому доказуванню в кримінальному провадженні (С. І. Хом’яченко, Т. О. Часова).

2. Констатовано, що на дисертаційному рівні висвітлення змісту електронних доказів зосереджено в роботах О. Ю. Гусєва («Електронні докази у цивільному процесі України», 2021), А. В. Скрипника («Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні», 2021), І. Г. Каланчі («Докази електронної форми у кримінальному процесі України: теорія та практика», 2025). Попри різні бачення науковців щодо поняття, значення, класифікації та інших аспектів електронних доказів, у працях останніх років простежується спільна думка про те, що докази в електронній формі мають особливу природу, яка відрізняє їх від традиційних матеріальних доказів, і це обґрунтовує їх самостійне місце в системі процесуальних джерел доказів.

3. Визначено, що оригіналом електронного технічного документа є той, який створений та зберігається на первинному носії інформації, натомість дублікатом (копією) є його копіювання, переміщення, поширення на інші носії даних. Акцентовано, що роздруківка вебсторінки, частини відео, фото чи іншого файлу не можуть бути визнані ні оригіналом, ні копією електронного документа та не мають самостійного доказового значення. Візуалізована в паперовій формі сторінка може бути тільки додатком до проведеної слідчої (розшукової) дії. Зауважено, що належне виготовлення дубліката

електронного документа забезпечує його допустимість під час перевірки доказів у суді.

4. Окреслено питання, що потребують врегулювання, стосовно використання електронних доказів у кримінальному процесуальному праві України, серед яких: невідмежованість електронного доказу від інших джерел доказів; невизначеність джерел одержання електронних доказів у кримінальному провадженні; недостатність нормативно-правового регулювання щодо застосування копії електронних доказів, оригінали яких утрачено; обмеження можливостей дізнавача стосовно застосування електронних доказів; неорганізованість роботи інформаційно-телекомунікаційної системи досудового розслідування за участю Національної поліції України.

5. На підставі дослідження міжнародного досвіду (Австрія, Болгарія, Велика Британія, Італія, Китайська Народна Республіка, Німеччина, Португалія, США, Чехія, Франція, Швеція) з'ясовано, що в більшості країн електронні дані визнають повноцінним видом доказів, рівнозначним традиційним письмовим чи речовим доказам, незалежно від наявності спеціального визначення в національному законодавстві. З'ясовано, що хоча законодавство переважної більшості досліджуваних країн не містять специфічного закону про електронні докази в кримінальному процесі, зарубіжна правозастосовна практика фокусує увагу на важливості дотримання принципу незмінності даних (жодного редагування оригіналу), документування всіх дій з електронним носієм і використання належних методів цифрової криміналістики, дотримання встановлених процесуальних вимог і технічних стандартів, щоб гарантувати автентичність і цілісність даних.

6. Акцентовано на браку уніфікованого міжнародного підходу до поняття, класифікації чи процедур поводження з електронними доказами, що ускладнює їх транскордонний обіг. У зв'язку з цим позитивно оцінено міжнародні акти ЄС (Регламент (ЄС) 2023/1543 про Європейські ордери на

пред'явлення та збереження електронних доказів у кримінальному провадженні та Директиву (ЄС) 2023/1544), що набувають чинності 2026 року та передбачають можливість для судових органів однієї країни безпосередньо звертатися з європейським ордером до інтернет-сервіс провайдера, який діє на території іншої країни, без необхідності проходження традиційного міждержавного запиту; визначають категорії даних, які можуть запитувати (дані абонента, дані трафіка й контент); встановлюють гарантії захисту прав у вигляді вимоги щодо повідомлення держави – виконавця ордера, яка може відмовити у виконанні за певних обставин (наприклад, якщо це загрожує національним інтересам або суперечить основним правам). Тобто ці міжнародні документи спрощують й уніфікують доступ до електронних доказів у межах Європейського Союзу, усуваючи залежність від повільних процедур взаємної правової допомоги.

7. З'ясовано, що відповідно до практики ЄСПЛ збирання та оцінка електронних доказів передбачають дотримання права на повагу до приватного й сімейного життя. Питання порушення такого права слід розглядати з позиції «розумного очікування конфіденційності». Висвітлено основні позиції ЄСПЛ у частині досліджуваного питання, відповідно до яких: 1) у сферу захисту права, передбаченого ст. 8 Конвенції, потрапляють не лише особисті відносини, а й різноманітні аспекти цифрових комунікацій (телефонні дзвінки, електронні листи, повідомлення, відомості про користування інтернетом на робочому місці тощо); 2) будь-яка форма цифрового нагляду повинна мати чітке законодавче підґрунтя та відповідати критеріям передбачуваності (моніторинг цифрових комунікацій без жодного нормативного акта чи внутрішньої політики не відповідає «вимозі передбаченості закону»); 3) втручання має бути необхідним у демократичному суспільстві, мати законну мету («охорона національної безпеки, запобігання злочинам, захист прав жертв») і бути пропорційним обставинам («серйозність злочинів й обмежений характер спостереження»).

РОЗДІЛ 2
ПРАВОВІ ПІДСТАВИ ТА ПОРЯДОК ДОСЛІДЖЕННЯ ДОКАЗІВ З ПОЗИЦІЇ ЇХ НАЛЕЖНОСТІ Й ДОПУСТИМОСТІ

2.1. Належність електронних доказів у кримінальному провадженні

Розвиток цифрових технологій призвів до того, що інформацію дедалі частіше зберігають і передають в електронній формі. У сучасних кримінальних провадженнях важливе значення мають електронні докази – дані на цифрових носіях, у мережі Інтернет чи інших електронних середовищах, які можуть підтверджувати обставини вчинення правопорушень. Водночас українське кримінальне процесуальне законодавство історично було зорієнтоване на традиційні види доказів (показання, речові докази, документи, висновки експертів) і не містило чітких норм щодо нових цифрових форм інформації. Це породжує проблему правової невизначеності: слідчим, прокурорам і суддям доводиться за аналогією застосовувати старі норми до нових явищ, що не завжди забезпечує ефективність і справедливість правосуддя. Постала потреба у визначенні на законодавчому рівні статусу електронних доказів, умов їх належності (доречності до справи) і допустимості (отримання законним шляхом), а також у розробленні спеціальних процесуальних правил їх збирання, перевірки й оцінки. Питання набуває особливої гостроти з огляду на необхідність дотримання балансу між ефективним розслідуванням (що вимагає оперативного отримання електронних даних) і забезпеченням прав людини, зокрема права на приватність та справедливий судовий розгляд.

Проблематику електронних доказів у кримінальному процесі активно досліджують останніми роками. Зокрема, В. Романюк і С. Абламський розглядали критерії допустимості цифрових доказів у контексті їх технічної специфіки та законодавчих прогалин [85, с. 140–142]. С. Р. Тагієв привернув

увагу до відсутності згадки про електронні докази серед джерел доказів у КПК України й обґрунтував необхідність законодавчого закріплення цього поняття [104, с. 5–7]. А.-М. Ю. Ангеленюк проаналізувала судові рішення в Україні щодо оцінки електронних доказів, розглянувши різні підходи судів до їх правової оцінки [3, с. 27–29]. Крім того, питанню використання електронних документів у доказуванні присвячено монографічне дослідження А. Гутника та А. Хитрої, які розкрили криміналістичні та процесуальні аспекти цієї проблематики [27, с. 11–15]. Отже, науковий інтерес до теми постійно посилюється, хоча єдності в підходах і термінології поки немає. Дослідники пропонують різні дефініції (цифрові, електронні, комп'ютерні докази) і дискутують, чи є такі докази самостійним видом чи різновидом традиційних джерел. Це засвідчує актуальність подальшого дослідження та формування узгоджених підходів.

Електронними доказами в широкому значенні вважають будь-яку інформацію в електронній (цифровій) формі, що може бути використана як доказ у кримінальному провадженні. Це можуть бути файли (документи, зображення, аудіо, відео), збережені на комп'ютерах, смартфонах, серверах або в хмарних сховищах; дані мережі Інтернет (вміст вебсайтів, дописи в соцмережах); електронне листування (e-mail, повідомлення в месенджерах); записи камер відеоспостереження; дані із систем GPS тощо. Відмітна риса такої інформації – відсутність самостійної матеріальної форми, вона існує у вигляді цифрового коду на певному носії або в мережі «coe.intcoe.int». Через цю нематеріальну природу постають питання, як ототожнити «оригінал» електронного доказу, забезпечити його цілісність й автентичність під час збору та передання до суду.

Своєю чергою, на думку опитаних правозастосувачів (97,6 %), доцільним видається законодавче закріплення таких видів електронних доказів, як абонентські дані, трафік-дані й контент-дані. Це засвідчує наявність запиту практики на законодавчу конкретизацію розуміння електронних доказів у кримінальному судочинстві.

КПК України наразі не містить визначення електронного доказу й не відносить його до переліку джерел доказів. Відповідно до ч. 2 ст. 84 КПК України, процесуальними джерелами доказів є показання, речові докази, документи й висновки експертів. Електронні носії чи дані безпосередньо не зазначені в цьому переліку [104, с. 5–6]. Отже, електронні докази в кримінальному процесі де-юре розглядають не як окремий вид, а крізь призму вже наявних категорій. З позиції сучасної доктрини електронний доказ поєднує два складники: зміст (цифрова інформація) і форму (електронний носій інформації). Тому електронний доказ може бути в кримінальному провадженні або документом (коли акцент на зафіксованій інформації), або різновидом речового доказу – якщо розглядати фізичний носій (комп'ютер, телефон тощо) як об'єкт, що містить інформацію. Зокрема, А. Гутник й А. Хитра зазначають, що в умовах законодавчого закріплення лише чотирьох джерел доказів цифрові (електронні) докази фактично доводиться відносити або до документів, або до речових доказів [27, с. 45–47]. Науковці наполягають, що електронні докази суттєво відрізняються від традиційних документів чи речей за своєю природою, тому потребують виокремлення в самостійний процесуальний інститут [104, с. 6–7].

Попри відсутність дефініції, певні норми КПК України все-таки застосовні до електронних доказів. Ключовою є ст.99 КПК, яка дає визначення документа як матеріального об'єкта, що містить зафіксовані відомості (текст, звук, зображення тощо) і може бути доказом факту або обставини. Частина 2 цієї статті уточнює, що до документів можуть належати, зокрема, матеріали фото-, відеозйомки, звукозапису й інші носії інформації (комп'ютерні дані) за умови, що вони містять необхідні відомості [53]. Отже, закон відносить комп'ютерні дані до різновиду документів. Важливо, що ч. 3 ст. 99 КПК визначає: оригіналом електронного документа є його електронне відображення, якому надано такий самий статус, як паперовому документу. Частина 4 ст. 99 КПК України встановлює, що дублікат документа, виготовлений тим самим способом, що й оригінал, а також копії інформації,

зокрема комп'ютерних даних, виготовлені слідчим чи прокурором із залученням спеціаліста, суд визнає оригіналом документа [53]. Ці норми запроваджено для полегшення використання електронних доказів: закон прирівняв належно виготовлені копії цифрових даних до оригіналу, аби сторона обвинувачення могла подавати їх без вилучення фізичного носія.

Окрім КПК, значення мають положення спеціального Закону України «Про електронні документи та електронний документообіг». Відповідно до ст. 7 цього Закону, якщо електронний документ зберігають на кількох носіях, кожен електронний примірник вважають оригіналом. Також один і той самий електронний документ може існувати на різних носіях, і всі екземпляри, ідентичні за змістом, розглядають як оригінали. Ця норма усуває проблему «оригіналу» цифрового документа – фактично всі автентичні копії рівноцінні. У судовій практиці це відображено в правовій позиції, що не може заперечувати допустимість електронного документа лише на тій підставі, що він має електронну форму. Об'єднана палата Касаційного кримінального суду (ОП ККС) Верховного Суду в постанові від 29 березня 2021 року зазначила, що електронний документ не можна дискримінувати порівняно з паперовим: його форма не є підставою для невизнання доказом [3]. Отже, закон і суди керуються принципом функціональної рівності електронних і традиційних доказів: за умови належної процедури збирання та збереження інформації, цифрові дані мають ту саму доказову силу, що й інші види доказів.

Важливим кроком стало внесення змін до КПК України Законом від 15 березня 2022 року № 2137-IX. Цей Закон, спрямований на підвищення ефективності розслідування кіберзлочинів «за гарячими слідами» та протидію кібератакам, упровадив низку новацій. Зокрема, уточнено порядок тимчасового вилучення та арешту електронних інформаційних систем і їх частин (зміни до ст. 170 КПК) [104]. Важливо, що законодавець спробував розмежувати електронну інформацію як доказ і пристрої як носії. У ч. 3 ст. 98 КПК (у редакції проєкту № 2740, який частково відображено в Законі № 2137-IX) пропонувалося закріпити, що інформація в електронному вигляді може

бути визнана речовим доказом, якщо вона є знаряддям, засобом або предметом злочину чи містить сліди злочину; водночас пристрої (комп'ютери тощо) не визнають речовими доказами, якщо вони лише містять інформацію [30, с. 76–84]. Хоча відповідні положення в остаточній редакції набули іншого вигляду, загальна тенденція зрозуміла: законодавець прагне мінімізувати вилучення техніки, зосередившись на електронних даних. Такий підхід має запобігти зловживанням, коли під приводом збору доказів органи слідства масово вилучали комп'ютери та сервери підприємств, паралізуючи їх роботу [30, с. 47–53]. Нині ж правоохоронці мають використовувати інструменти копіювання даних, дампінгу інформації тощо, залишаючи оригінальні пристрої власникам, якщо ті не є знаряддям злочину.

Проаналізуємо критерії належності й допустимості електронних доказів. Електронні докази, як і будь-які інші, повинні відповідати загальним критеріям доказування: належності, допустимості, достовірності й достатності.

Загалом питання належності доказів як складової процесуальних властивостей доказів вивчали у своїх наукових доробках такі науковці, як: Г. П. Власова і Р. В. Сафроняк [13], В. В. Головчук [24], В. О. Малярова [56], Д. Б. Сергєєва [90], В. В. Сичевський [91], М. М. Стоянов [101] та ін. У науковій доктрині належність доказів розглядають як їх придатність встановлювати обставини, що є предметом доказування, через логічний зв'язок між отриманими фактами й обставинами, які підлягають доказуванню або мають значення для кримінального провадження, обставинами, що підтверджують достовірність чи недостовірність, можливість чи неможливість використання інших доказів [24]. Згідно із законодавчими положеннями належність означає, що доказ стосується предмета доказування, тобто підтверджує чи спростовує обставини, які мають значення для кримінального провадження (ст. 85 КПК).

У контексті електронних доказів це означає, що цифрові дані мають прямо чи опосередковано стосуватися злочину: наприклад, листування

повинно мати зв’язок зі злочинними діями, а не бути сторонньою інформацією. Допустимість передбачає отримання і подання доказу відповідно до процесуального закону. Для електронних доказів питання допустимості є надзвичайно актуальним, оскільки порушення порядку збору цифрової інформації (відсутність санкції суду на обшук чи доступ до даних, порушення прав власника інформації, збої під час вилучення носіїв тощо) можуть стати підставою для визнання доказу недопустимим. Дослідники зауважують, що складність забезпечення допустимості цифрових доказів пов’язана з їхньою технічною природою: потрібні спеціальні знання та засоби, щоб коректно вилучити дані без спотворення, задокументувати цей процес і підтвердити автентичність отриманої інформації [85, с. 141–143]. В. В. Романюк і С. Є. Абламський доводять, що цифрові докази мають складну структуру, тому їх процесуальне «легалізування» потребує чітких критеріїв: підтвердження джерела походження, цілісності файлів, належної фіксації під час слідчих дій тощо [85, с. 144–147]. Достовірність електронного доказу означає його правдивість, тобто відсутність спотворень даних. Цей аспект тісно пов’язаний з технічною автентичністю: чи відповідає файл тому, яким він був у момент події. Для забезпечення достовірності застосовують методи підтвердження автентичності – електронні підписи, контрольні хеш-суми, залучення експертів для встановлення відсутності змін у файлах [3, с. 28–30]. Достатність – це оцінка сукупності доказів, на підставі яких можна дійти висновків у справі; окремі електронні докази зрідка бувають самодостатніми, здебільшого вони доповнюють інші матеріали, створюючи цілісну картину.

Розглянемо специфіку збирання та зберігання електронних доказів (ланцюг custody). Особливість електронних доказів полягає в тому, що їх нескладно змінити або знищити непомітно, а процес копіювання не залишає видимих слідів (на відміну від, скажімо, копіювання паперового документа). Тому критично важливо дотриматися правильного порядку збирання, перевірки та зберігання цифрових доказів – так званого ланцюга збереження

доказу (chain of custody). Міжнародні стандарти рекомендують фіксувати кожен етап роботи з електронним доказом: хто, коли і як його виявив, отримав (скопіював), хто мав доступ до носія чи файлу, як забезпечували його захист від змін. Будь-яка зміна або втрата даних можуть поставити під сумнів допустимість і достовірність доказу. Рада Європи в Electronic Evidence Guide (2022) акцентує, що для гарантії прийнятності електронних доказів у суді слід забезпечити їх автентичність: простежуваність походження та цілісність на всіх стадіях поводження з ними [134, с. 15–17]. З позицій практики це означає, що під час обшуку чи огляду комп'ютерної техніки бажано залучати спеціаліста або експерта, який зробить цифрову копію (зліпок диска, дамп пам'яті тощо) з фіксацією контрольних сум. Оригінальний носій варто опечатувати і зберігати, мінімізуючи до нього доступ. Копію використовують для аналізу, а оригінал – як еталон для перевірки. Такий підхід дає змогу згодом довести в суді, що представлений файл є тим самим, який був вилучений на місці події та не зазнав прихованого редагування. Недотримання цих вимог може мати наслідки: захист майже напевно заявить клопотання про визнання доказу недопустимим, якщо буде принаймні найменший сумнів щодо його цілісності або законності отримання.

Українські суди поступово розробляють підходи до оцінки електронних доказів. Верховний Суд 2021 року підтвердив, що електронна форма носія не може бути підставою для відмови в доказі. В іншій постанові ОП ККС ВС від 25 вересня 2023 року (справа № 208/2160/18) було узагальнено критерії оцінки електронних доказів на стадії судового розгляду [27, с. 73–75]. Зокрема, суд вказав на необхідність перевіряти: (1) чи дотримано процедури отримання інформації (наприклад, чи був дозвіл суду на тимчасовий доступ до даних або обшук гаджета); (2) чи підтверджено автентичність файлів (наприклад, наявність електронного підпису, сертифіката, висновку експерта щодо незмінності файлу); (3) чи надано стороні захисту можливість оглянути оригінал носія або копію з нього [3, с. 27–29]. Якщо ці умови виконано,

електронний доказ вважають допустимим, його оцінює суд за внутрішнім переконанням нарівні з іншими доказами.

Практика Європейського суду з прав людини зосереджує увагу на питанні доказів переважно з позицій справедливості судового розгляду (ст. 6 Конвенції). Принципова позиція ЄСПЛ полягає в тому, що питання допустимості доказів належать до компетенції національних судів, а завдання Страсбурзького суду – оцінити, чи було провадження справедливим загалом. Використання незаконно отриманих доказів (зокрема електронних даних, здобутих без дозволу, шляхом порушення права на приватність тощо) не автоматично означає порушення права на справедливий суд. ЄСПЛ перевіряє, чи мала сторона захисту достатні можливості оспорити такий доказ, чи оцінювали національні суди обставини його отримання, чи не став цей доказ вирішальним єдиним доказом вини. Наприклад, у рішенні «Хан проти Великої Британії» [143] ЄСПЛ хоча й констатував порушення права на приватне життя через прослуховування, проте не побачив порушення справедливого суду, оскільки заявник міг заперечувати проти запису, а суди ретельно зважили всі обставини. В інших справах ЄСПЛ зауважував, що ключовими є якість доказів і відсутність примусу до їх отримання [126]. Якщо електронний доказ було здобуто з порушенням права на приватність (ст. 8 Конвенції), суд оцінюватиме, чи це порушення підірвало справедливість процесу. У справі «Биков проти Росії» було використано запис розмови, зроблений таємно без належного дозволу; ЄСПЛ визнав, що хоча здійснено втручання в приватність, у цьому випадку воно не порушило ст. 6, оскільки заявник міг оскаржити автентичність запису і в справі були інші докази [141]. Отже, стандарт ЄСПЛ полягає в перевірці дотримання балансу: чи не було право сторони захисту поставлене в нерівні умови використанням електронного доказу, чи не було отримання цього доказу пов’язане з грубим порушенням інших прав (наприклад, катуваннями, що завжди робить доказ неприйнятним), і чи оцінені національними судами надійність та вирішальність такого доказу. Досвід ЄСПЛ, а також практика іноземних держав (США, країни ЄС) засвідчують

необхідність урівноважувати інтереси правосуддя та права людини під час поводження з електронними доказами.

В інших країнах питання допустимості електронних доказів вирішують по-різному, але простежуються спільні тенденції. У Європейському Союзі останніми роками прийнято низку нормативних актів, спрямованих на спрощення отримання електронних доказів у транскордонному вимірі. Зокрема, 2023 року затверджено Регламент (ЄС) 2023/1543 і Директиву 2023/1544, які встановлюють єдині процедури для судових органів країн-членів щодо доступу до електронних даних, які зберігаються в іншій державі [88]. Зазначене має підвищити ефективність розслідування в цифровому середовищі, водночас ці акти містять гарантії захисту персональних даних і правоособливостей користувачів (вимоги ордерів, контроль суду запитуваної країни тощо). У низці держав (США, Велика Британія, Німеччина) розроблено доктрини «найкращого доказу» для електронної інформації, які вимагають надавати суду оригінальні носії або достовірно засвідчені копії, а будь-які сумніви в автентичності трактують на користь обвинуваченого. У деяких юрисдикціях створено детальні цифрові протоколи для правоохоронців – інструкції, як діяти з електронними пристроями під час обшуку, як документувати дії з ними, як зберігати дані. Наприклад, рекомендації ФБР або Європолу з криміналістики електронних пристроїв регламентують, що слід першочергово ізолювати пристрій від мережі (щоб віддалено не знищили дані), зробити копію тільки для читання, обчислити контрольну суму (hash) і порівнювати її на всіх етапах, щоб виявити будь-яку зміну [134, с. 22–25]. Іноземний досвід підтверджує: електронні докази не повинні бути ні дискриміновані, ні привілейовані, порівняно з іншими видами доказів. Їх оцінку здійснюють за тими самими критеріями релевантності та достовірності, проте з огляду на технічні особливості. Для України, яка знаходиться на шляху євроінтеграції, урахування цих стандартів є вкрай важливим [5, с.15–17].

На рівні практики українських судів питання належності електронних доказів часто зводиться не стільки до змісту даних, скільки до їхнього чіткого

зв’язку з предметом доказування. Для листування в месенджерах ключовим є контекст: ідентифікація користувача (прив’язка акаунта до конкретної особи), часові «прив’язки» (метадані), спосіб здобуття (тимчасовий доступ чи обшук пристрою), а також логіка ланцюга подій – чи відображає листування планування, підготовку або завершення злочину, чи є лише «тлом» спілкування. Для відеозаписів вирішальними є місце встановлення камери, неперервність запису й відсутність ознак монтажу; для «онлайнових» артефактів (скриншоти, вебсторінки) – спосіб фіксації (протокол огляду з фіксацією URL і часу, використання вебархівів, технічних логів) і підтвердження незмінності. Рада Європи пропонує «мінімальний стандарт» належності: цифрові дані мають бути ідентифіковані (зв’язок із користувачем/пристроєм/акаунтом), локалізовані (місце/сховище/сервіс), прив’язані в часі (timestamp/метадані) й відтворювані (можливість отримати перевірну копію) [134, с. 15–17; 22–25]. У такому підході належність перетворюється на перевірювану властивість цифрових даних [134, с. 15–17].

Об’єднана палата Касаційного кримінального суду в постанові від 29 березня 2021 року у справі № 554/5090/16-к зауважила: електронний формат не є підставою для відмови в допустимості; закон про електронні документи прирівнює належно відтворені електронні екземпляри до оригіналу [124, с. 5–6]. Це має прямі наслідки для належності: якщо в електронному файлі містяться фактичні відомості, релевантні предмету доказування, він prima facie належний; далі суд переходить до перевірки допустимості – як саме дані здобуто та чи збережено їх цілісність. У новіших рішеннях ОП ККС ВС (25 вересня 2023 року № 208/2160/18) акцентовано на триєдиному тесті для цифрових матеріалів: законність доступу/вилучення, підтвердження автентичності (електронний підпис, сертифікат, висновок експерта, хеш-суми) і забезпечення рівності сторін (можливість огляду копії або оригіналу стороною захисту) [63].

ЄСПЛ послідовно зауважує, що питання допустимості віднесено до сфери національного права, а завдання Страсбурга – оцінити, чи було

провадження справедливим загалом (ст. 6 Конвенції). У справі «Khan v. the United Kingdom» Суд визнав, що таємний аудіозапис становив втручання у приватність, але немає автоматизму: вирішальним є те, чи мав обвинувачений реальну можливість спростувати доказ, чи зважили національні суди на обставини його отримання і чи не став цей доказ єдиною вирішальною підставою для вироку [126; 143]. Практичний висновок для національних судів такий: навіть за наявності застережень до «маршруту» отримання цифрових даних окремо оцінюють їх якість (автентичність, повноту), контрадикторність (можливість ефективного оспорення) і значущість у сукупності [126; 143]. Цей підхід узгоджується з українськими тестами належності, допустимості й достовірності.

Транскордонний вимір належності формалізовано пакетом e-Evidence: Регламент (ЄС) 2023/1543 і Директива (ЄС) 2023/1544 (OJ L 191 від 28 липня 2023 року) запроваджують European Production Order (EPOC) і European Preservation Order (EPOC-PR) для отримання та збереження електронних даних у провадженнях із транскордонним елементом [132; 149]. Для належності це важливо, по-перше, тому що EPOC «прив'язує» запит до конкретних процесуальних обставин (категорії даних, часові межі, ідентифікатори акаунтів), формалізуючи релевантність; по-друге, Директива 2023/1544 зобов'язує провайдерів призначати правових представників у державах-членах для оперативного виконання запитів, що мінімізує втрати даних і підвищує відтворюваність доказу [132]. Для України, яка отримує чи запитує дані від провайдерів ЄС, урахування цих механізмів у міжнародній правовій допомозі посилює і належність (точність предмета запиту), і допустимість (прозорий правовий маршрут отримання) [133].

Сучасні наукові роботи пропонують практичні «чек-листи» для збереження автентичності: фіксація джерела (user/device/account), ізоляція пристрою від мережі, створення форензичних образів у режимі «тільки для читання», розрахунок і збереження хеш-сум до/після копіювання, ведення журналу доступів, використання робочої копії для аналізу зі збереженням

еталонного образу для верифікації в суді [134, с. 22–25]. Українська доктрина 2024–2025 років слушно зауважує: без таких технічних етапів суд об’єктивно позбавлений інструментів для перевірки автентичності; якщо немає хеш-ідентифікаторів чи принаймні експертного підтвердження незмінності файлів, сумнів тлумачать на користь обвинуваченого [3, с. 28–30; 63, с. 302–305; 85, с. 144–147]. Це безпосередньо стосується й належності: доказ, який неможливо об’єктивно ототожнити з подією, особою або часом, втрачає зв’язок із предметом доказування.

З огляду на типові ситуації можна окреслити кілька практичних орієнтирів для слідчого, прокурора й суду. У справах, що ґрунтуються на даних месенджерів і соцмереж, належність підвищують: технічні довідки провайдерів або власників платформ; зіставлення з даними операторів (CDR, геолокації); «подвійне джерело» – огляд пристрою і тимчасовий доступ до хмарного сховища [134, с. 23–25]. Для відео та CCTV поряд із записом доцільно витребувати журнали подій відеореєстратора, схему розміщення камер, технічну інструкцію до системи, а за можливості – верифікувати час запису (NTP-синхронізація) [124, с. 6–7]. Для OSINT/вебконтенту потрібні огляди з фіксацією URL, часу (UTC), checksum архіву сторінки (WARC), а також можливість незалежної верифікації (webarchive); необхідно чітко зазначати, яку саме обставину підтверджує фрагмент і як він пов’язаний із підозрюваним [88, с. 2–3]. Для електронних документів із КЕП необхідно перевіряти ланцюжок сертифікатів та їхній статус на момент підписання; у разі експорту – долучати технічні звіти перевірки до процесуальних документів [53; 63].

Доцільно також узгодити кримінально-процесуальний підхід із напрацюваннями суміжних галузей: ЦПК, ГПК і КАС виокремлюють електронні докази як самостійний вид. Нові публікації 2025 року пропонують адаптувати цю логіку для КПК: визнати «електронний доказ» процесуальним джерелом sui generis, визначити загальні дефініції та базові вимоги до форми,

змісту і джерел [63, с. 302–305]. Це послабить поточне напруження вибору між «документом» і «річчю» та забезпечить передбачуваність кваліфікації.

Електронні докази стали невіддільною частиною сучасного кримінального процесу у зв’язку з глобальною цифровізацією. Вони охоплюють широкий спектр електронної інформації – від текстових файлів й електронних листів до записів камер спостереження та даних з мережевих ресурсів. Аналіз засвідчив, що національне законодавство України поки що не визначає електронні докази як окреме процесуальне джерело, проте чинні норми (ст. 84, 99 КПК тощо) дають змогу залучати цифрові дані до доказової бази, трактуючи їх як документи або речові докази. Останні зміни (закон № 2137-IX) сигналізують про поступове усвідомлення законодавцем специфіки електронних доказів і необхідності окремого регулювання порядку роботи з ними. Водночас зберігаються прогалини й неузгодженості, що підтверджують дискусії в науці та розбіжності в практиці.

Електронним доказам притаманні ті самі фундаментальні вимоги, що й традиційним: вони повинні бути належними до справи та допустимими з погляду закону. Водночас їхня допустимість безпосередньо залежить від дотримання специфічних умов збирання та обробки: отримання із законного джерела (за рішенням суду, з добровільної згоди власника даних або в інший передбачений спосіб), забезпечення цілісності інформації (відсутності несанкціонованих змін), документування кожного кроку роботи із цифровим носієм. Практика засвідчує, що найвразливішим місцем є саме технічна сторона: якщо сторона обвинувачення не може переконливо довести автентичність файлу (наприклад, навести хеш-значення, яке збігається з оригіналом, або пред’явити оригінальний носій для перевірки), суд схиляється трактувати сумнів на користь обвинуваченого й відхилити такий доказ. Тому в роботі з електронними доказами слід застосовувати високий стандарт ретельності, бажано із залученням експертів.

Українські суди поступово формують підходи до оцінки електронних доказів, акцентуючи, що цифрові докази не можна відхилити лише через їхню

форму, і визнаючи копії електронних документів за належної процедури оригіналами. Європейський суд з прав людини не висуває окремих жорстких правил щодо електронних доказів, але його прецеденти засвідчують необхідність справедливого балансу: права сторони захисту не має бути порушено через використання електронного доказу, отриманого із сумнівним дотриманням прав. У кожному випадку важливо оцінити, чи не було порушено базові права (приватність, право не свідчити проти себе тощо) під час здобуття такого доказу, чи мав обвинувачений можливість ефективно його оскаржити. Якщо електронний доказ став результатом грубого порушення прав, це може поставити під сумнів увесь процес.

На підставі здійсненого аналізу можна сформулювати такі пропозиції. По-перше, необхідно на законодавчому рівні закріпити визначення електронного (цифрового) доказу як самостійного джерела з відповідними правилами поводження з ним. Слід внести зміни до ст. 84 КПК, доповнивши перелік джерел доказів категорією електронних доказів, а також детально врегулювати процедури вилучення, копіювання та засвідчення електронної інформації. По-друге, слід розробити підзаконні нормативні акти або офіційні методичні рекомендації для слідчих і судів щодо роботи із цифровими доказами. Це можуть бути інструкції на основі міжнародного досвіду (наприклад, рекомендації Ради Європи), які встановлюватимуть стандарти фіксації та зберігання електронних даних. По-третє, доцільно підвищувати рівень технічної оснащеності та кваліфікації правоохоронних органів у галузі комп’ютерної криміналістики, щоб забезпечити належну реалізацію нових норм на практиці. По-четверте, необхідно врахувати європейські тенденції щодо співпраці у сфері електронних доказів: імплементувати положення актів ЄС, що стосуються транскордонного отримання даних, адже чимало злочинів мають міжнародний компонент (сервери чи акаунти знаходяться за кордоном).

Тож належність електронних доказів у кримінальному провадженні забезпечують за умови, якщо такі докази отримано і представлено відповідно до закону та з огляду на критерії доказовості. Електронні докази не є ні

другорядними, ні «особливими» – вони мають відповідати тим самим принципам, що й інші, але методи роботи з ними повинні враховувати специфіку цифрових даних. Визнання електронних доказів повноцінним складником доказової бази – виклик сучасності, на який правова система України має відповісти шляхом оновлення законодавства і практики в контексті найкращих міжнародних стандартів, забезпечуючи й ефективність правосуддя, і захист основоположних прав людини.

2.2. Допустимість електронних доказів у кримінальному провадженні

На сучасному етапі розвитку суспільства вчинення кримінальних правопорушень супроводжується застосуванням цифрових (електронних) засобів, унаслідок чого, з одного боку, їх використовують злочинці, а з іншого – слідчі для збирання доказів, які також мають цифрову (електронну) форму. Однією з обов'язкових характеристик доказової інформації в кримінальному провадженні є її допустимість, завдяки чому (у разі відповідності іншим вимогам) вона набуває власне значення доказу. У зв'язку із цим на практиці правильне розуміння допустимості цифрових (електронних) доказів, складників цього поняття та їхнього впливу на процедуру збирання доказів є вкрай важливим.

Окремі аспекти допустимості доказів у кримінальному провадженні досліджували В. В. Вапнярчук [8], О. В. Капліна [42], О. В. Крикунов та Г. В. Денісова [52], Є. Д. Лук'янчиков та Б. Є. Лук'янчиков [55], Ю. Л Мельничук [60], О. П. Метелев [61], А. В. Панова [68], М. А. Погорецький [72; 75], Д. Б. Сергєєва [89], В. А. Смирнов [96], О. С. Степанов [99], В. В. Тютюнник [106], І. Л. Чупрікова [119] та інші вчені.

Порядок використання електронних доказів та їх статус у кримінальному процесуальному праві України, зауважує А.-М. Ангеленюк,

мають бути детально врегульовані в законодавстві. Утім слід констатувати недостатність такого регулювання та наявність прогалин права щодо питань, які стосуються електронних доказів у кримінальному процесі [2, с. 215].

На відміну від звичайних паперових документів, характеристики та просторові межі яких можна бачити, електронні документи мають іншу природу та вирізняються такими характеристиками:

– електронний документ не може бути без носія інформації. Значущими є ідентифікаційні властивості носія інформації (зокрема найменування типу, марки моделі, індивідуального машинного носія, на якому записано документ);

– електронні докази не видимі для «неозброєного ока» (без спеціального інструментарію), для їх сприйняття та дослідження застосовують програмно-технічні засоби;

– вони можуть бути змінені, пошкоджені або знищені в процесі експлуатації пристрою користувачем чи під впливом фізичних чинників (високий рівень вологості, висока температура, електромагнітні випромінювання тощо);

– за стадіями виготовлення документи, зокрема електронні, поділяють на оригінали, дублікати, копії та виписки. У ч. 3 ст. 99 КПК України зазначено, що оригіналом документа є власне документ, а оригіналом електронного документа – його відображення, якому надають таке саме значення, як і документу. Проте для електронного документа такі поняття, як «оригінал», «дублікат», «копія», є умовними, тому що в усіх цих випадках електронний документ залишається оригіналом.

Джерелами доказів в електронній формі можуть бути: різні носії інформації; моноблоки, мобільні пристрої (мобільні телефони, планшетні комп’ютери), цифрові камери, роутери, маршрутизатори, комп’ютерні мережі, глобальна мережа Інтернет, звуко- та відеозаписи тощо, тобто джерелом доказів може бути будь-який електронний пристрій, який є на місці обшуку.

Слід зауважити, що постійно з’являються новітні види електронних пристроїв, які можуть містити електронні докази. Нині, і це вже очевидно, коли розглядають традиційні злочини, зважають на ймовірність наявності електронних доказів. Тому під час досудового розслідування з’ясовують, чи має потерпілий від злочину комп’ютер, чи підтримує він інтернет-контакти тощо. Докази вчинення злочину можуть знаходитися в: комп’ютері потерпілого; інтернет-провайдера, послугами якого користувався потерпілий; комп’ютері підозрюваного; інтернет-провайдера, послугами якого користувався підозрюваний; іншому місці кіберпростору. Важливим джерелом доказів є комп’ютерна система, що складається з корпусу, де розміщені мікропроцесор, плати, накопичувачі інформації та порти для зовнішніх пристроїв; монітора; периферійних пристроїв (принтер, сканер тощо), програмного забезпечення, зокрема: системне програмне забезпечення; прикладне програмне забезпечення (текстові та графічні редактори, системи управління базами даних, електронні таблиці, системи презентацій тощо). До інформаційних об’єктів (даних) належать: текстові та графічні документи; дані у форматах мультимедіа; інформація у форматах баз даних й інші додатки прикладного характеру [11].

Істотну інформацію можуть містити й тимчасові файли. Більшість текстових редакторів і систем управління базами даних створює тимчасові файли як побічний продукт нормальної роботи програмного забезпечення. Користувачі комп’ютерів не розуміють вагомості створення цих файлів тому, що їх знищує програма наприкінці сеансу роботи. Однак дані, які мають ці знищені файли, можуть виявитися найважливішими, передусім якщо вихідний файл був зашифрований чи документ із текстом був надрукований без збереження на дисках, такі файли можуть бути відновлені.

Вирізняють зовнішні та внутрішні накопичувачі інформації, а також змінні носії (CD, DVD диски), різні USB-накопичувачі. У цифрових камерах і мобільних телефонах активно застосовують невеликі за розмірами карти

пам’яті (SD, micro SD, compact Flash CF тощо), які можуть мати значний обсяг інформації.

Наприклад, карта Western Digital SanDisk Ultra microSDXC має обсяг пам’яті 400 ГБ. Чимало різної інформації містять теперішні мобільні пристрої – смартфони, планшети та різні плеєри. Крім того, інформацію про факти й обставини, що є значущими для кримінального провадження, можуть мати системи відеоспостереження. Необхідно зауважити, що в IP-камерах можуть бути накопичувачі даних, що надають можливість робити відеофіксацію та зберігати відеоматеріал без підключення до реєстратора. Більшість електронних пристроїв можуть здійснювати обмін інформацією через локальні комп’ютерні мережі або глобальну мережу Інтернет. Тому для дослідження спеціалізованих пристроїв (концентраторів, маршрутизаторів, комутаторів тощо) потрібні знання фахівця. Слід зважати на те, що значний обсяг інформації зберігається у «хмарних технологіях», тобто поза місцезнаходженням фізичної чи юридичної особи. Для перевірки цілісності інформації застосовують механізм розрахунку контрольної суми або хеш-суми. Контрольна сума – певне значення, обчислене на основі набору даних із використанням одного з математичних (криптографічних) алгоритмів (наприклад, CRC32, MD5, SHA-1, SHA-2, SHA-3 тощо), які застосовують для перевірки цілісності даних під час їх передачі або збереження [11].

Зазначені контрольні суми можна одержати, послуговуючись, наприклад, такою програмою, як HashTab (у відкритому доступі в мережі Інтернет), яку вважають найефективнішою для цього.

В. В. Петрик зауважує, що в теперішньому кримінальному процесі застосування електронних доказів стає істотним інструментом у доказуванні винуватості чи невинуватості обвинуваченого. З розвитком інформаційних технологій та цифровізації суспільства значення електронних доказів, таких як файли, листування, відео та аудіозаписи, дані з мобільних пристроїв, а також інші форми цифрової інформації, істотно підвищилося. Такі докази можуть мати вирішальне значення для підтвердження фактів, що є значущими для

кримінального провадження, а також для ефективного розслідування правопорушень, передусім в умовах, коли традиційні методи збору доказів не є достатньо ефективними [70, с. 119].

На думку опитаних правозастосувачів, основними критеріями допустимості електронних (цифрових) доказів є: належне документування процесу отримання (33,3 %), законність отримання (26,2 %), автентичність даних (19 %), цілісність даних (16,7 %).

Узагальнюючи викладене, зауважимо, що процес збирання, дослідження та оцінки електронних доказів, на нашу думку, має передбачати дотримання таких фундаментальних положень:

1) законність передбачає, що всі дії щодо виявлення, фіксації, вилучення та дослідження електронних доказів слід здійснювати виключно в межах, у спосіб і відповідно до чинного законодавства, загальних процесуальних та криміналістичних принципів;

2) цілісність даних. Дії фахівця не мають призводити до матеріальних змін інформації, електронних пристроїв чи носіїв інформації, які можуть застосовувати як докази;

3) документування процесу. Документують будь-які дії, виконувані щодо електронних доказів, зберігають ці документи на випадок перевірки, щоб незалежна третя сторона мала можливість повторити ці дії та одержати аналогічний результат;

4) експертна підтримка. Якщо передбачено, що під час огляду (обшуку) можуть бути виявлені електронні докази, залучають підтримку фахівців (спеціалістів), забезпечивши, за можливості, їх присутність на місці події;

5) відповідна фахова підготовка. Якщо під час огляду (обшуку) немає фахівців з електронних доказів, першочергові дії на місці події виконують особи, які мають необхідні знання та навички для виявлення та збирання доказів;

6) розумна обережність передбачає уникнення будь-яких навмисних або ненавмисних дій, що можуть призвести до пошкодження потенційних доказів, представлених у цифровій формі.

Наприклад, правоохоронці не повинні мати доступ до цифрових пристроїв, якщо їм бракує компетентності й вони не обізнані з відповідними процесами, а саме якщо фізичний обсяг цифрового пристрою достатньо великий, наприклад, сервер в інформаційному центрі, чи це критично для безпеки цифрового пристрою, зупинка якого загрожуватиме життю людей, або коли потрібно зафіксувати спосіб роботи підозрюваного під час зловживання системою [11, с. 5–9].

За стадіями виготовлення електронні документи поділяють на оригінали, дублікати, копії та витяги. Проте вважаємо, що цей поділ є доволі умовним.

У ч. 3, 4 ст. 99 КПК міститься визначення, що є оригіналом і дублікатом документа. Сторона кримінального провадження, потерпілий, представник юридичної особи, стосовно якої здійснюють провадження, зобов'язані дати суду оригінал документа. Оригіналом документа є власне документ, а оригіналом електронного документа – його відображення, якому надають такого самого значення, як документу [53].

Дублікат документа (документ, зроблений у такий самий спосіб, як і його оригінал), а також копії інформації, зокрема комп'ютерних даних, що містяться в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, судом визначає як оригінал документа [53].

Для підтвердження змісту документа можуть бути визнані допустимими й інші відомості, якщо:

1) оригінал документа втрачений або знищений, крім випадків, якщо він втрачений або знищений з вини потерпілого або сторони, яка його дає;

2) оригінал документа не може бути одержаний за допомогою доступних правових процедур;

3) оригінал документа знаходиться в користуванні однієї зі сторін кримінального провадження, а вона не надає його на запит іншої сторони.

Сторона кримінального провадження, потерпілий, представник юридичної особи, стосовно якої здійснюють провадження, мають право надати витяги, компіляції, узагальнення документів, які незручно повністю досліджувати в суді, а на вимогу суду – зобов'язані надати документи в повному обсязі.

Сторона зобов'язана надати іншій стороні змогу побачити або скопіювати оригінали документів [53].

Отже, оригіналом електронного технічного документа є той, що створений та зберігається на первинному носії інформації. Наприклад, оригінал відеозапису з камер відеоспостереження зберігається на носії інформації, на який записують відео. Дублікатом (копією) такого відеозапису є його копіювання, переміщення, поширення на інший носій даних.

Ми вважаємо, що роздруківка вебсторінки, частини відео, фото чи іншого файлу не може бути визнано ні оригіналом, ні копією електронного документа та самостійно не може бути застосована як доказ. Візуалізована в паперовій формі сторінка може бути застосована тільки як додаток до проведеної слідчої (розшукової) дії. Належне виготовлення дубліката електронного документа забезпечує його допустимість під час перевірки доказів у суді.

Слід погодитись з А. В. Ратновою, яка не поділяє думку, що відмінностей в електронних документах, якими можна було б обґрунтувати виділення будь-яких електронних документів (наприклад, аудіо- та відеозаписів) у самостійний підвид, немає, оскільки несуттєво, яка інформація (текст, відеозапис, аудіозапис тощо) записана на машинному носії. Електронні документи за формою можна поділити на відеозаписи, аудіозаписи, електронні повідомлення, вебсайти й інформацію в електронній формі. Під час

аналізу судової практики встановлено, що часто суди досліджують такий вид електронного доказу, як відеозапис. Це можуть бути як відеозаписи з подією здійснення злочину, так і відеозаписи зі слідчими діями, слідчими експериментами тощо. Також є випадки вивчення судом аудіозапису (телефонних розмов з повідомленням про злочин, аудіозапис із плачем дитини та звуками ударів тощо). Крім того, трапляються випадки дослідження скриншотів електронних сторінок з листуванням [84].

С. А. Чванкін стверджує, що аудіо- та відеозаписи повноцінно ввійшли до складу судових доказів і вже протягом тривалого проміжку часу їх активно застосовують у процесі судового доказування. Близько 90 % інформації про навколишній світ більшість людей сприймає через зір, ще близько 9 % – за допомогою слуху [116].

Теоретичне та практичне значення класифікації електронних документів полягає в тому, що вона дає змогу правильно застосовувати їх як докази, допомагає збиранню, перевірці (вивченню їх для встановлення наявності чи відсутності ознак втручання) та оперуванню ними в доказуванні під час розслідування і судового розгляду [84, с. 43–44].

На думку С. Тагієва, актуальність питання використання електронних доказів у кримінальному судочинстві обумовлена новітніми методами передачі даних і, як наслідок, новими технологіями вчинення кримінальних правопорушень. Місце та роль електронних доказів у кримінальному процесі чітко не визначені, їх розглядають у кримінальному процесуальному законі фрагментарно, тому що з моменту їх появи минув порівняно нетривалий проміжок часу. Безперечним фактом є те, що зміни, які відбуваються в суспільному житті, впливають на розслідування кримінальних проваджень. У зв’язку з цим органи дізнання, досудового слідства та судові органи в кримінальних провадженнях активно застосовують електронну інформацію, що своєю чергою вимагає дослідження проблемних питань правового регулювання застосування електронних доказів у кримінальному процесі [104, с. 5].

О. І. Марочкін зауважує, що невпинний технічний прогрес зумовлює необхідність пошуку оптимальних шляхів адаптації законодавства до сучасних реалій. Такі тенденції безпосередньо стосуються сфери кримінального судочинства, у якій цифровізація виявляється в різноманітних аспектах. Одним із них є застосування електронних доказів у кримінальному провадженні. Запровадження цієї категорії в кримінальний процес ускладнюється браком належного нормативного регулювання, різноманітністю поглядів науковців стосовно цього питання, а також постійним удосконаленням технічних засобів зберігання та передання інформації [57, с. 107].

У національній кримінальній процесуальній доктрині виокремлюють такі критерії допустимості доказів: 1) належне джерело отримання доказів; 2) належний суб'єкт; 3) належний спосіб збирання доказів [27, с. 75–89]. Розглянемо їх детальніше.

1. Належне джерело отримання доказів. Кримінальний процесуальний кодекс України визначає, що процесуальними джерелами доказів є показання, речові докази, документи та висновки експертів (ч. 2 ст. 84).

Нині практика боротьби зі злочинністю має керуватися положеннями кримінального процесуального законодавства України, а отже, формальним їх розумінням як різновиду документів, зокрема як електронного документа.

Стаття 99 КПК України закріплює офіційний термін «документ» як джерело доказу, а саме визначає його як спеціально створений для збереження інформації матеріальний об'єкт, що містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо певні відомості, що можуть бути використані як доказ фактів чи обставин, які встановлюють під час кримінального провадження [53].

Окрім цього, зазначена стаття містить конкретизований перелік документів, які можуть бути доказами в кримінальному процесі: матеріали фотозйомки, звукозапису, відеозапису й інші носії інформації (зокрема

електронні), на яких за допомогою технічних засобів зафіксовано процесуальні дії.

Деякі науковці стверджують, що, з огляду на законодавче закріплення тільки чотирьох джерел доказів, джерелом цифрових (електронних) доказів є документ або речовий доказ (річ). Для того щоб відрізнити електронний документ від речового доказу в електронній формі, необхідно зважати на те, що саме може бути використано як доказ факту чи обставин, які встановлюють під час кримінального провадження – інформацію чи матеріальний об'єкт [27, с. 83]. Ця теза видається спірною, тому що доказом не може бути матеріальний об'єкт, доказом завжди є інформація, яку містить певний матеріальний об'єкт як її носій.

Точне визначення джерела цифрового (електронного) доказу є запорукою використання правильного засобу та процедури фіксації й вилучення доказової інформації, її збереження відповідно до визначених КПК України правил. Крім того, під час роботи із джерелами цифрових (електронних) доказів, пошуку таких доказів, їх фіксації та вилучення обов'язково слід залучати відповідних спеціалістів, що гарантуватиме належність виконання зазначених завдань.

2. Належний суб'єкт збирання цифрових (електронних) доказів. Вимога про те, що цифровий (електронний) доказ має бути одержаний належним суб'єктом, означає отримання його таким учасником кримінального провадження, який є правомочним здійснювати це провадження або ж окрему процесуальну дію. Належним суб'єктом, уповноваженим на проведення досудового розслідування, є слідчий або дізнавач, визначений керівником органу досудового розслідування для здійснення конкретного кримінального провадження (ч. 1 ст. 214 КПК України). Слід також ураховувати, що в разі якщо слідчому із заяви, повідомлення чи інших джерел стало відомо про обставини, які можуть свідчити про здійснення кримінального правопорушення, розслідування якого не віднесено до його компетенції (підслідності), він проводить розслідування доти, доки прокурор не визначить

іншу підслідність (ч. 2 ст. 218 КПК України) [53]. У такому разі слідчий або дізнавач є належними в цьому кримінальному провадженні до моменту визначення підслідності прокурором.

Ця особливість є актуальною під час розслідування кримінальних правопорушень, що вчиняють через мережу Інтернет. У більшості випадків місця здійснення таких кримінальних правопорушень визначають за місцем реєстрації або проживання потерпілих, так встановлюють і територіальну підслідність. Проте згодом, після встановлення місця перебування (проживання) підозрюваної особи, постає необхідність зміни територіальної підслідності та передачі матеріалів кримінального провадження в порядку ст. 218 КПК України. Наприклад, після проведення низки процесуальних дій за IP адресою було встановлено пристрій, з якого злочинець здійснив шахрайські дії. Тож місцезнаходження цього пристрою і буде місцем здійснення кримінального правопорушення [53].

Слід ураховувати, що під час вирішення питання стосовно підслідності в кожному випадку надходження зазначеної інформації слідчий у порядку ст. 218 КПК України впродовж п’яти днів з дня її одержання письмово повідомляє прокурора та продовжує здійснювати досудове розслідування доти, доки прокурор не визначить іншу підслідність.

Уповноваженим на здійснення окремих процесуальних дій слід також вважати слідчого (дізнавача):

− якому постановою слідчого іншого органу досудового розслідування іншої територіальної юрисдикції чи прокурора доручено проведення слідчих (розшукових) і негласних слідчих (розшукових) дій (ч. 6 ст. 218 КПК України);

− який входить до складу слідчої групи (п. 1 ч. 2, ч. 4 ст. 39 КПК України) або спільної слідчої групи (ст. 571 КПК України);

− який на час провадження конкретних слідчих (розшукових) чи інших процесуальних дій, у результаті яких було отримано докази, перебував на посаді слідчого й виконував свої трудові обов’язки (зокрема, не перебував на лікуванні, у відпустці тощо).

Крім того, до цього переліку можна додати ситуації, коли процесуальні дії вчиняє прокурор (процесуальний керівник у кримінальному провадженні) відповідно до п. 4 ч. 2 ст. 36 КПК України та коли такі дії здійснює оперативний працівник за дорученням слідчого (дізнавача) або прокурора відповідно до ч. 2 і 3 ст. 41 КПК України.

Однак на практиці виникають проблеми. Наприклад, згідно зі ст. 160 КПК України, сторони кримінального провадження мають право звернутися до слідчого судді під час досудового розслідування чи суду під час судового провадження з клопотанням про тимчасовий доступ до речей і документів [53].

Законодавець визначив вичерпний перелік осіб, які мають право звертатися з відповідним клопотанням, і недотримання цієї вимоги закону є підставою для відмови в задоволенні клопотання. Подавати відповідне клопотання повинен саме той слідчий, який здійснює досудове розслідування в кримінальному провадженні, у межах якого таке клопотання подають. У разі ж заміни слідчого в кримінальному провадженні разом із клопотанням слід подавати докази про це, чим може слугувати постанова про призначення нового слідчого. У разі ж якщо досудове розслідування здійснює група слідчих (слідча група), а клопотання підписує один із них, то слід додавати постанову про призначення групи слідчих у цьому кримінальному провадженні. Це правило стосується і прокурора, який погоджує відповідне клопотання або подає його самостійно. Іншим прикладом є факт звернення з відповідним клопотанням не слідчим, а оперуповноваженим, який не є учасником кримінального провадження, а тому йому не може бути надано тимчасовий доступ до речей і документів. Порушення цієї вимоги може призвести до відмови слідчого судді в задоволенні клопотання.

3. Належний спосіб збирання цифрових (електронних) доказів. Дослідники здебільшого вважають, що процес доказування є триступеневим і полягає в збиранні, перевірці й оцінці доказів. Збирання доказів, тобто їх одержання, слід проводити відповідно до спеціально встановленої процедури. Її дотримання гарантує їх допустимість, що означає можливість їх

використання в межах кримінального провадження. Аналіз положень ст. 93 КПК України надає можливість виокремити такі законні способи збирання доказів стороною обвинувачення [53]:

− надання доказів добровільно учасником кримінального провадження (отримання);

− витребування доказів;

− проведення тимчасового доступу до електронного документа (як заходу забезпечення);

− проведення слідчих (розшукових) дій (огляд, обшук);

− проведення негласних слідчих (розшукових) дій.

Після одержання електронного документа на носії інформації слідчий, дізнавач зобов'язані оглянути його.

Зі свого боку сторона захисту, потерпілий та його представник можуть збирати електронні документи шляхом: 1) одержання чи витребування їх від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових і фізичних осіб; 2) ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій стороною обвинувачення. У контексті права сторони захисту, потерпілого на ініціювання проведення процесуальних дій учасники є лише ініціаторами, а суб'єктами збирання в разі задоволення клопотання буде слідчий, дізнавач або прокурор.

Під час розслідування кримінальних правопорушень, сліди вчинення яких мають цифровий (електронний) характер, типовим є застосування таких процесуальних засобів, як витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових і фізичних осіб речей, документів, тимчасового доступу до речей і документів. Кримінальний процесуальний кодекс України визначає певний порядок реалізації цих процесуальних дій, порушення якого призводить до недопустимості зібраних доказів.

Наприклад, під час зверненні до суду з клопотанням про тимчасовий доступ до речей та документів слідчі іноді не виконують вимоги ч. 2 ст. 93 КПК України. Зокрема, у деяких випадках слідчі, попри надані їм повноваження, безпосередньо не звертаються до фізичних і юридичних осіб з метою одержання зазначених у їхніх клопотаннях документів, а в судовому засіданні не доводять, що речі або документи, до яких просять надати доступ, знаходяться або можуть знаходитися у володінні відповідно фізичної чи юридичної особи [53].

Аналіз судової практики з розгляду клопотань зазначеної категорії також свідчить про те, що слідчі судді виносять ухвали про відмову в задоволенні клопотань про надання тимчасового доступу до речей і документів через недоведеність обґрунтування значення конкретних речей та документів для встановлення обставин у кримінальному провадженні, а також з підстав недоведеності органом досудового розслідування того, що тільки шляхом вилучення оригіналів документів можливе з'ясування певних обставин, на які орган досудового розслідування посилається в клопотанні [85, с. 144–146].

Відповідно до ст. 162 КПК України, до охоронюваної законом таємниці, яка міститься в речах і документах, серед іншого належать відомості, що можуть становити банківську таємницю, особисте листування особи й інші записи особистого характеру, а також інформація, яку мають оператори та провайдери телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, зокрема отримання послуг, їх тривалості, змісту, маршрутів передавання тощо. Такі дані становлять інтерес для слідства здебільшого в процесі розслідування справ про шахрайство, вчинене з використанням інформаційно-комунікаційних технологій, адже за допомогою розкриття цих даних здійснюють ідентифікацію особи злочинця.

За результатами аналізу судової практики, під час подання клопотань про тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю (банківська, інформація про зв'язок абонента тощо), слідчі

не завжди належно обґрунтовують неможливість іншими способами довести обставини, які передбачено довести за допомогою цих речей і документів (ч. 6 ст. 163 КПК України) [53].

Ми поділяємо думку Н. М. Ахтирської, що розвиток науки й техніки створив необмежені можливості для цивілізаційного розвитку, водночас спричинив виникнення серйозних загроз для неї. Цифровізація, комп'ютеризація, електронний документообіг і банкінг, інформаційні бази даних стали зручним інструментом нинішнього світу, однак статистичні показники дають підстави стверджувати, що загрозливими темпами збільшується кількість злочинів, які здійснюють із застосуванням інформаційних технологій [6, с. 142].

Електронні документи за стадіями виготовлення поділяють на оригінали, дублікати, копії та витяги. За комбінацією метаданих електронні документи можуть бути поділені на однорангові, дворангові, трирангові, чотирирангові, п'ятирангові. Залежно від доступу до метаданих їх можна поділити на електронні документи з відкритими та прихованими метаданими. За ступенем захисту виокремлюють електронні документи відкриті та закриті. За джерелом походження є документи, створювані користувачем і комп'ютерною системою. Класифікацію електронних документів можна здійснити за їх розміщенням: комп'ютер, смартфон, планшет, відеокамера, «розумна» побутова техніка, інтернет-сервер тощо. Електронні документи за формою можна поділити на відеозаписи, аудіозаписи, електронні повідомлення, вебсайти. Систематизація критеріїв класифікації електронних документів дає змогу розробити тактику збирання, перевірки й оцінки електронних документів, удосконалити криміналістичну методику розслідування деяких видів кримінальних правопорушень, у яких доказами можуть бути електронні документи [84].

Складність розв'язання проблеми допустимості цифрових (електронних) доказів пов'язана з тим, що вони мають складну технічну природу. Насамперед зазначене зумовлено тим, що цей різновид доказів має

абстрактні технічні й математичні моделі, вирізняється специфічними умовами виникнення, існування, копіювання та зберігання, що відрізняє їх від інших видів доказової інформації.

Суттєвим для практики є чітке розуміння критеріїв, за якими цифрова (електронна) інформація може набувати значення доказу в кримінальному провадженні. З огляду на це визначено та висвітлено такі критерії допустимості доказів: 1) належне джерело отримання доказів; 2) належний суб'єкт; 3) належний спосіб збирання доказів.

2.3. Взаємозв'язок допустимості й належності доказів і стандартів доказування

Оцінка доказів є центральним елементом кримінального процесуального доказування. Вона передбачає встановлення належності, допустимості й достовірності кожного доказу, а також достатності їх сукупності для прийняття процесуальних рішень. Водночас достатність доказів не може існувати ізольовано від належності й допустимості, адже лише їх поєднання забезпечує законність, обґрунтованість висновків органів досудового розслідування та суду.

Важливе значення ця проблематика має у зв'язку з необхідністю застосування стандартів доказування. Такі стандарти, як «обґрунтована підозра», «достатня підстава» та «поза розумним сумнівом», призначені визначати поріг достатності доказів залежно від процесуальної стадії та характеру рішення, яке ухвалюють. Проте в національній доктрині комплексне дослідження взаємозв'язку належності, допустимості й достатності доказів зі стандартами доказування досі не здійснювали.

Теоретичні та практичні аспекти оцінки доказів і визначення їх достатності аналізували М. В. Дєєв [30], О. В. Капліна [42], С. О. Ковальчук [45], С. М. Стахівський [97], М. М. Стоянов [102],

О. Г. Шило [120], М. Є. Шумило [121] та ін. Проблематику стандартів доказування в кримінальному провадженні висвітлювали В. В. Вапнярчук [10], І. В. Гловюк [22], В. А. Завтур [33], Г. Р. Крет [50], М. А. Погорецький [73; 74; 76], Х. Р. Слюсарчук [95], А. С. Степаненко [98], О. М. Толочко [105]. Попри посилену увагу до обох категорій, їх взаємозв'язок у контексті кримінального процесуального доказування вивчено недостатньо, що зумовлює актуальність цього дослідження.

Достатність доказів у кримінальному провадженні – це наявність такої сукупності належних, допустимих і достовірних доказів, яка надає можливість дійти обґрунтованого висновку щодо певних обставин справи й ухвалити законне та вмотивоване процесуальне рішення. Вона є системною властивістю доказів, що відображає їхню якісну та кількісну відповідність завданням доказування [31].

Належність доказів визначає їх зв'язок з обставинами кримінального провадження, а допустимість – відповідність процесуальним нормам щодо форми та способу одержання. Якщо принаймні одного із цих критеріїв не дотримано, доказ втрачає процесуальне значення, що унеможливлює досягнення достатності. Тож належність і допустимість становлять підґрунтя для формування достатності доказів.

У кримінальному процесі застосовують різні стандарти доказування:

– «обґрунтована підозра» – мінімальний рівень доказової переконливості, необхідний для повідомлення особі про підозру або застосування запобіжного заходу;

– «достатня підстава» – проміжний стандарт, що вимагає ширшої сукупності доказів для ухвалення процесуальних рішень, зокрема під час передачі справи до суду;

– «поза розумним сумнівом» – найвищий стандарт, який застосовує суд під час постановлення вироку, означає, що всі сумніви щодо вини особи усунуті об'єктивними доказами.

Залежно від стадії кримінального провадження достатність доказів виявляється в різних вимірах. Для повідомлення про підозру достатньо досягнення стандарту «обґрунтована підозра», для скерування обвинувального акта – «достатня підстава», а для постановлення обвинувального вироку – «поза розумним сумнівом».

Отже, достатність доказів є універсальною властивістю, яка виявляється в різному ступені залежно від застосовуваного стандарту доказування. Належність і допустимість слугують передумовою визнання доказів достатніми.

Згідно з ч. 1 ст. 94 КПК України, слідчий, прокурор, слідчий суддя та суд оцінюють докази за внутрішнім переконанням, що ґрунтується на всебічному, повному та неупередженому дослідженні всіх обставин кримінального провадження. Достатність доказів є системною властивістю, яка відображає наявність сукупності належних, допустимих і достовірних доказів на конкретний момент провадження з метою ухвалення відповідного процесуального рішення.

Водночас не всі процесуальні рішення потребують оцінки доказів з позицій достатності. Згідно з ч. 1 ст. 110 КПК України, процесуальними рішеннями є акти органів досудового розслідування, прокурора, слідчого судді та суду, проте лише ті з них, що передбачають оцінку сукупності доказів, вимагають формування внутрішнього переконання в наявності чи відсутності підстав для їх ухвалення.

У доктрині виокремлюють дві групи підходів: стандарти як об’єктивні правила, що визначають якість та кількість доказів, і стандарти як суб’єктивний рівень переконання суб’єкта доказування.

Належність і допустимість є вихідними критеріями, що забезпечують можливість урахування доказу в процесі доказування. Якщо доказ не відповідає цим критеріям, він не може формувати достатність, а отже, не здатний бути основою для досягнення відповідного стандарту доказування.

Кожен стандарт доказування відображає різний ступінь достатності доказів:

- для повідомлення про підозру – «обґрунтована підозра»;
- для направлення обвинувального акта до суду – «достатня підстава»;
- для постановлення обвинувального вироку – «поза розумним сумнівом».

Усі ці рівні ґрунтуються на попередньому визнанні доказів належними та допустимими. Допустимість і належність формують передумову для встановлення достатності доказів, а остання – умову для досягнення відповідного стандарту доказування.

Аналіз наукових позицій дає підстави стверджувати, що стандарти доказування поєднують як об’єктивний, так і суб’єктивний критерії.

З позицій об’єктивного критерію стандарти доказування відображають закріплені в КПК України та судовій практиці Верховного Суду правила, які визначають вимоги до кількості та якості доказів. Вони задають орієнтири для оцінки доказів з огляду на ч. 2 ст. 91 та ч. 1 ст. 94 КПК України. Стандарти доказування, слушно зауважує Г. Р. Крет, охоплюють не лише кількісні та якісні вимоги, а й правила формування достатньої сукупності належних, допустимих і достовірних доказів [92].

З позицій суб’єктивного критерію стандарти доказування відображають рівень внутрішнього переконання, достатній для ухвалення процесуального рішення. Він формується внаслідок усебічного й повного дослідження доказів, їх оцінки та узгодження з конкретними обставинами справи.

У кримінальному процесі належність означає зв’язок доказу з обставинами, що підлягають доказуванню, а допустимість – його отримання у спосіб, передбачений законом. Недотримання принаймні одного з цих критеріїв унеможливлює врахування доказу під час ухвалення рішення. Отже, лише належні й допустимі докази можуть становити основу для формування достатності.

Система стандартів доказування в кримінальному провадженні охоплює три ключові рівні: «обґрунтована підозра», «достатня підстава» та «поза розумним сумнівом». Їх спільною рисою є орієнтованість на оцінку сукупності доказів, яка має відповідати певному рівню переконливості.

Достатність доказів набуває конкретного змісту залежно від застосовуваного стандарту. Якщо для повідомлення про підозру достатньо обґрунтованого припущення, то для вироку необхідна абсолютна переконливість, яка усуває всі розумні сумніви.

Г. Р. Крет зауважує, що стандарт «поза розумним сумнівом» є нормативно закріпленим правилом, що визначає рівень достовірності знань про обставини справи, необхідний для постановлення вироку [51]. Його застосовують виключно на завершальному етапі провадження, коли суд вирішує питання про винуватість чи невинуватість особи.

Цей стандарт вимагає, щоб знання про факт вчинення кримінального правопорушення ґрунтувалося на сукупності належних, допустимих і достовірних доказів, оцінених у межах всебічного, повного та неупередженого дослідження. Ідеться не лише про кількісну достатність, а й про якісну переконливість, яка унеможливлює будь-які розумні сумніви у винуватості.

Отже, достатність доказів забезпечує дотримання цього стандарту завдяки підтвердженню на основі фактичних даних достовірного висновку про вчинення кримінального правопорушення.

Традиційно в науці кримінального процесу поняття «докази» залишається дискусійним, що породжує різні тлумачення. У загальній теорії процесуального права доказами розглядають будь-які фактичні дані, отримані у встановленому порядку, що підтверджують або спростовують обставини справи.

Згідно зі ст. 84 КПК України, доказами в кримінальному провадженні є фактичні дані, одержані в передбаченому законом порядку, на підставі яких уповноважені суб’єкти встановлюють наявність чи відсутність обставин, що

мають значення для кримінального провадження. До процесуальних джерел доказів належать показання, речові докази, документи та висновки експертів.

Тож доказами є дані, які достовірно відображають події минулого й можуть бути використані для встановлення об'єктивної істини.

Належність визначає, наскільки доказ пов'язаний із предметом доказування та чи здатний він підтвердити чи спростувати певну обставину. Допустимість означає відповідність доказу процесуальним вимогам щодо способу його отримання.

Відсутність належності або допустимості унеможливлює врахування доказу під час оцінки його достатності, оскільки такий доказ не має юридичної сили. Саме ці критерії формують базу для подальшого застосування стандартів доказування.

Достатність доказів означає таку їх сукупність, яка надає можливість уповноваженим суб'єктам сформувати внутрішнє переконання щодо обставин кримінального провадження. Вона є проміжною категорією між процесуальними властивостями доказів (належністю та допустимістю) і стандартами доказування.

Отже, достатність є сполучною ланкою, без якої неможлива реалізація стандартів доказування на практиці.

Використання кожного зі стандартів безпосередньо залежить від наявності достатньої сукупності належних і допустимих доказів.

Предметом доказування в кримінальному процесі розуміють сукупність обставин, що підлягають встановленню в кримінальному провадженні для його правильного вирішення [145, с. 226]. Оскільки розслідування концентрується навколо злочину, дослідженню мають підлягати його ознаки, властивості й елементи.

Докази в цьому контексті відіграють визначальну роль. Законодавство не лише визначає поняття доказів, а й регламентує порядок їх отримання, перевірки й оцінки [118]. Це забезпечує об'єктивність кримінального процесу та реалізацію принципу верховенства права.

Однією з ключових гарантій захисту прав людини в кримінальному процесі є визнання недопустимими тих доказів, що отримані з порушенням кримінального процесуального закону. У науковій літературі допустимістю доказів вважають здатність джерела відомостей формувати факти, які мають юридичне значення [92, с. 168]. Відповідно до ст. 86 КПК України, доказ визнають допустимим лише в разі, якщо він одержаний у процесуально встановленому порядку.

До критеріїв допустимості, на наш погляд, слід віднести:

1) процесуальна компетенція суб'єкта, який здійснює слідчі чи процесуальні дії;

2) надійність фактичних даних, що становлять зміст доказу;

3) дотримання вимог процесуальної форми;

4) етичність тактичних прийомів отримання доказів [145, с. 224].

Отже, допустимість забезпечує правову «чистоту» доказів і є запобіжником проти свавілля органів досудового розслідування.

Належність доказів визначають їхнім змістовим зв'язком із предметом доказування. Доказ вважають належним, якщо він безпосередньо чи опосередковано підтверджує або спростовує факти, що мають значення для кримінального провадження (ст. 85 КПК України).

Належність гарантує, що до доказової бази не буде включено факти, які не мають відношення до справи, і водночас забезпечує концентрацію уваги на юридично значущих обставинах.

Важливе місце інститут допустимості доказів посідає в Конституції України. У ч. 3 ст. 62 Основного Закону закріплено, що обвинувачення не може ґрунтуватися на доказах, одержаних незаконним шляхом, а також на припущеннях [49]. Це положення підкреслює фундаментальну роль допустимості в гарантуванні прав людини та справедливості судового розгляду.

Визначення належності й допустимості доказів є передумовою застосування стандартів доказування, які є своєрідним «мірилом» рівня переконливості доказової бази:

– стандарт «обґрунтованої підозри» вимагає мінімальної сукупності належних і допустимих доказів для притягнення особи до кримінального провадження;

– стандарт «достатньої підстави» передбачає вищий рівень обґрунтованості для ухвалення проміжних процесуальних рішень (наприклад, застосування запобіжних заходів чи проведення негласних слідчих дій);

– стандарт «поза розумним сумнівом» є найвищим рівнем доказової переконливості й обов'язковою умовою для постановлення обвинувального вироку [31; 35].

Питання допустимості та належності доказів у кримінально-процесуальній науці розглядають як одне з вихідних положень теорії судових доказів. Належність визначають як здатність доказу підтверджувати чи спростовувати обставини, що належать до предмета доказування, натомість допустимість – як дотримання процесуальної форми й умов отримання доказів, встановлених законом.

Згідно зі ст. 86 КПК України, доказ визнають допустимим лише за умови його отримання в порядку, визначеному кримінальним процесуальним законодавством. Водночас належність доказів передбачає їх зв'язок із предметом доказування, тобто з фактичними обставинами кримінального правопорушення.

Правильне визначення допустимості та належності доказів істотно впливає на перебіг усього процесу доказування – від збирання й перевірки доказової інформації до її оцінки судом. Неправильна оцінка допустимості доказів може призвести не лише до помилок у розслідуванні злочинів, а й до формування недовіри суспільства до правоохоронних органів і правосуддя загалом.

Конституція України (ч. 3 ст. 62) прямо встановлює, що обвинувачення не може ґрунтуватися на доказах, одержаних незаконним шляхом, а також на припущеннях. Це положення відображає фундаментальну ідею: допустимість є гарантією дотримання прав і свобод особи.

Стандарти доказування («обґрунтована підозра», «достатня підстава», «поза розумним сумнівом») відображають рівень переконливості й достовірності знання, необхідного для ухвалення конкретного процесуального рішення. Їх реалізують виключно за умови використання доказів, що є належними й допустимими [117, с. 258].

Стандарт «поза розумним сумнівом» вимагає, аби сукупність доказів була достатньою та переконливою настільки, щоб виключати розумні сумніви у винуватості обвинуваченого. Будь-який недопустимий або неналежний доказ підриває можливість досягнення цього стандарту.

Несформованість єдиного підходу до інституту допустимості й належності доказів спричиняє низку проблем у практиці. Зокрема, дискусійними залишаються питання щодо юридичної сили доказів, отриманих із порушенням процесуальної форми, а також їх можливого використання у виняткових випадках.

Науковці обґрунтовують, що неналежне чи незаконне отримання доказів безпосередньо позначається на рівні гарантій прав людини в кримінальному процесі. Тож інститут допустимості й належності потребує подальшого осмислення, узагальнення теоретичних напрацювань і вдосконалення процесуального законодавства.

Поняття належності в національній доктрині відображає зв’язок доказу з предметом доказування. Це означає, що доказ визнають належним лише за умови, якщо він здатен підтвердити або спростувати обставини, які належать до кола юридично значущих фактів. Отже, належність є своєрідним фільтром, який відсікає матеріали, що не мають прямого чи опосередкованого стосунку до справи.

Водночас належність не є категорією, яку можна оцінювати ізольовано від контексту. На практиці значення мають не тільки формальні зв'язки доказу з фактом, а й здатність цього доказу наблизити суд до встановлення істини. Інколи навіть побічні відомості, які, на перший погляд, не стосуються предмета доказування, у системному поєднанні з іншими матеріалами утворюють логічний ланцюг, що дає змогу суду сформувати переконання.

У теоретичному вимірі належність можна тлумачити в кількох площинах. По-перше, вона має онтологічний аспект, адже встановлює об'єктивну здатність доказу відображати факт, що має правове значення. По-друге, вона має епістемологічний аспект, оскільки спрямована на визначення того, наскільки певний доказ, поєднаний з іншими, може забезпечити переконливе пізнання істини. Зрештою, належність має і нормативний вимір, адже оцінку цього критерію завжди здійснюють крізь призму процесуальних норм, які визначають предмет доказування в конкретному виді судочинства [118, с. 983].

Слід зауважити, що належність не обмежується прямим, безпосереднім зв'язком між доказом і фактом. У низці випадків суди мають справу з так званими похідними чи побічними доказами, які не відображають факт безпосередньо, але дають підстави вивести висновок про його існування шляхом логічних операцій. Наприклад, у кримінальному процесі показання свідка, який бачив особу поблизу місця вчинення злочину, можуть мати значення для підтвердження її можливої причетності, хоча безпосередньо факт учинення злочину не встановлюють. У цивільному процесі квитанція про оплату послуг може бути побічним доказом наявності договірних відносин між сторонами.

Тож належність не завжди є категорією «чорно-білою». У практиці вона має градаційний характер, адже один і той самий доказ може бути більш чи менш релевантним залежно від контексту справи й сукупності інших наданих матеріалів. Судова практика сформувала підхід, за яким належність оцінюють не ізольовано, а у взаємозв'язку з усією доказовою базою.

Значуща особливість полягає і в тому, що належність доказу завжди визначають з огляду на предмет доказування. Саме коло фактів, які підлягають встановленню в конкретній справі, задає межі належності. У кримінальному провадженні предмет доказування визначений ст. 91 КПК України, де перелічено обставини, що мають значення для встановлення винуватості чи невинуватості особи. У цивільному процесі межі предмета доказування формуються нормами матеріального права, які регулюють спірні відносини. Це означає, що належність – категорія динамічна: залежно від правової кваліфікації чи зміни предмета позову один і той самий доказ може стати належним або втратити цю властивість.

З позицій порівняльного права критерій належності має універсальний характер і притаманний більшості правових систем. Наприклад, у системі загального права він відомий як принцип «relevance of evidence», його розглядають крізь призму його логічної здатності впливати на ймовірність істинності чи хибності факту. У континентальній правовій традиції акцентовано передусім на нормативному аспекті належності: чи належить певна обставина до предмета доказування, визначеного законом.

Оцінка належності нерозривно пов’язана з іншими характеристиками доказів – допустимістю та достовірністю. Проте, якщо допустимість передбачає перевірку джерела й способу отримання доказу, то належність відповідає на питання, чи має доказ юридичне значення в конкретному процесі. Своєю чергою достовірність визначає, чи можна довіряти змісту доказу. Тільки у взаємозв’язку цих характеристик формується повноцінна доказова база [145, с. 224].

Допустимість доказів пов’язана з дотриманням процесуальної форми їх одержання, закріпленої в законі. Це категорія, яка найбільше відображає баланс між ефективністю правосуддя та правами учасників процесу. Порушення правил щодо джерела, порядку збирання чи подання доказу автоматично призводить до його недопустимості, навіть якщо такий доказ містить об’єктивно істотну інформацію.

Допустимість нерозривно пов’язана з принципом верховенства права. Недопущення використання незаконно здобутих доказів спрямоване на захист людини від свавільного втручання держави. Тож допустимість є не лише технічною вимогою до доказового процесу, а й інструментом забезпечення довіри до судочинства.

Допустимість доказів – це фундаментальна категорія доказового права, яка визначає, чи може певний доказ бути використаний у процесі для підтвердження або спростування обставин, що мають юридичне значення. Її сутність полягає у відповідності доказу встановленим законом вимогам щодо джерела, способу одержання та процесуальної форми закріплення. Якщо ці вимоги порушені, доказ вважають недопустимим, він не може бути врахований судом під час ухвалення рішення, навіть якщо він об’єктивно містить істотну для справи інформацію.

З погляду історії ідея допустимості пов’язана з обмеженням державної влади у сфері доказування. Вона сформувалася як реакція на практики середньовічного інквізиційного процесу, коли для встановлення істини застосовували будь-які засоби, включно з катуваннями. У сучасних демократичних правопорядках аксіоматичним є принцип: доказ, здобутий з порушенням закону, не може бути використаний, оскільки це підриває ідею правосуддя.

Допустимість має кілька вимірів. Передусім це процесуально-правовий аспект, який визначає, чи отримано доказ уповноваженим суб’єктом у передбачений законом спосіб. Наприклад, у кримінальному процесі протокол обшуку визнають допустимим лише за умови, що він проведений на підставі відповідної ухвали суду або у випадках невідкладності, прямо передбачених законом. У цивільному та господарському судочинстві допустимість часто пов’язана з дотриманням правил форми письмових доказів, нотаріального посвідчення чи реєстрації правочинів.

Другий вимір – це правозахисний аспект, який відображає взаємозв’язок допустимості із фундаментальними правами людини. Використання доказів,

отриманих із порушенням права на приватність, права на захист або права не свідчити проти себе, є недопустимим, навіть якщо такі докази мають високу пізнавальну цінність. Отже, допустимість є механізмом втілення конституційних принципів у практику судочинства.

Третій вимір – це інституційний аспект, пов'язаний із довірою до судової системи. Суспільство сприймає судове рішення як справедливе не лише тоді, коли воно ґрунтується на істині, а й тоді, коли його ухвалено внаслідок чесної процедури. Відмова від використання недопустимих доказів створює передумови для того, щоб судочинство не було інструментом маніпуляцій або зловживань з боку держави чи окремих осіб.

У практиці Європейського суду з прав людини допустимість доказів розглядають крізь призму ст. 6 Конвенції про захист прав людини і основоположних свобод, яка гарантує право на справедливий суд. Суд не встановлює жорстких правил допустимості для держав, визнаючи, що вони мають певну свободу розсуду. Водночас він зауважує, що використання доказів, здобутих із грубим порушенням прав людини, не сумісне з принципом справедливого судочинства. Наприклад, у справах «Яллох проти Німеччини» чи «Шенк проти Швейцарії» Суд зазначив, що допустимість оцінюють не ізольовано, а з огляду на справедливість процесу загалом [92, с. 73].

Привертає увагу проблема співвідношення допустимості й об'єктивної істини. У наукових дискусіях часто порушують питання: чи справедливо відкидати доказ, який фактично підтверджує істину, лише тому, що його отримано із процесуальним порушенням. Прихильники жорсткого підходу акцентують, що допущення таких доказів створює небезпечний прецедент, легалізуючи порушення прав людини. Прихильники гнучкого підходу спрямовують увагу на ризик ухвалення помилкових рішень через відмову від урахування об'єктивно вагомої інформації. Українське право, як і більшість європейських систем, переважно дотримується першої позиції, з огляду на пріоритетність процедурної справедливості над досягненням матеріальної істини за будь-яку ціну.

Слід зазначити, що категорія допустимості має динамічний характер. Вона еволюціонує залежно від розвитку технологій, зміни соціальних уявлень про приватність і баланс інтересів особи й держави. Наприклад, поява цифрових доказів, даних із соціальних мереж, інформації з камер спостереження ставить нові виклики перед правовими системами. Те, що раніше не підлягало доказуванню або його вважали неможливим для використання, нині стає предметом оцінки на предмет допустимості. У цьому контексті важливе значення має чітке регламентування процедур доступу до цифрової інформації, аби зберегти баланс між ефективністю правосуддя та правами особи.

Стандарти доказування визначають рівень переконливості, необхідний для того, щоб суд визнав факт встановленим. Їхня природа поєднує логічний та ціннісний елементи. З одного боку, стандарт виражає об’єктивну потребу в певній кількості та якості доказів, з іншого – відображає аксіологічні орієнтири суспільства щодо справедливого балансу між інтересами особи та держави.

У кримінальному процесі класичною моделлю є стандарт «поза розумним сумнівом», який вимагає максимально високого рівня переконаності суду у винуватості особи. У цивільному та господарському процесах найчастіше застосовують стандарт «переваги доказів», що означає достатність того, щоб певна версія виглядала імовірнішою, порівняно з іншими. В адміністративному судочинстві інколи формують проміжний стандарт, що враховує специфіку публічно-правових спорів.

Стандарти доказування є однією з найскладніших і водночас найважливіших категорій доказового права. Вони визначають рівень переконливості, достатній для того, щоб суд визнав певний факт встановленим й обрав його за основу рішення. Тобто стандарт доказування – це критерій, за допомогою якого оцінюють, чи досягнуто того рівня впевненості, що дає змогу дійти правового висновку.

На відміну від таких характеристик доказів, як належність чи допустимість, стандарт доказування не стосується окремого доказу. Він охоплює всю сукупність доказової бази, встановлює межу, після подолання якої суд вважає факт доведеним. Отже стандарт виконує роль орієнтира для судової оцінки, забезпечуючи єдність і передбачуваність судової практики.

Належність і допустимість створюють базовий фундамент для формування доказової системи. Вони є передумовою можливості досягнення стандарту доказування. Суд, оцінюючи, чи досягнуто відповідного рівня переконливості, насамперед керується тими матеріалами, які пройшли «подвійну перевірку» на відповідність критеріям належності й допустимості.

Недопустимі докази, навіть якщо вони є об’єктивно цінними з позицій істини, не можуть бути враховані під час формування внутрішнього переконання суду. Це означає, що стандарт доказування ніколи не може бути досягнуто за допомогою незаконних доказів. Такий підхід інколи критикують як надто формалізований, але саме він гарантує баланс між завданням правосуддя і захистом прав людини.

З іншого боку, належність визначає релевантність доказу до стандарту доказування. Якщо матеріал не стосується обставин, які потребують встановлення, він не може наблизити суд до досягнення необхідного рівня переконливості. Отже, належність і допустимість формують своєрідну «рамку», у межах якої відбувається оцінка доказів на відповідність стандарту [51, с. 131].

У доказовому праві категорії належності й допустимості традиційно розглядають як первинні фільтри, які визначають, чи може конкретний доказ брати участь у формуванні переконання суду. Водночас стандарти доказування визначають кінцеву межу, подолання якої дає змогу суду визнати факт доведеним. Саме тому між цими категоріями є тісний і багатовимірний взаємозв’язок: належність і допустимість створюють підґрунтя для оцінки доказів, натомість стандарт доказування встановлює орієнтир для цієї оцінки.

Якщо в кримінальному процесі обвинувачення ґрунтується переважно на показаннях, отриманих під тиском або без адвоката, їх визнають недопустимими, суд зобов'язаний ігнорувати їх під час формування внутрішнього переконання. Унаслідок цього навіть очевидна з позицій життєвої логіки причетність особи до злочину може не бути підтвердженою в правовому сенсі через брак допустимих доказів.

Отже, допустимість є своєрідним бар'єром, який відокремлює правосуддя від свавільного використання незаконних методів. Її зв'язок зі стандартами доказування полягає в тому, що саме наявність достатньої кількості допустимих доказів є необхідною умовою для досягнення відповідного стандарту.

Належність забезпечує релевантність доказу до предмета доказування. Вона визначає, чи взагалі може інформація вплинути на переконливість сукупності доказів у справі. Якщо доказ не стосується юридично значущих обставин, він не здатний наблизити суд до досягнення стандарту. Наприклад, у цивільній справі про стягнення боргу документи, що підтверджують соціальний статус відповідача, не є належними, оскільки не дають відповіді на питання про наявність чи відсутність зобов'язання.

Водночас межі належності є доволі гнучкими. Один і той самий доказ у різному контексті може мати або не мати належності. Якщо предмет позову змінюється (наприклад, замість вимоги про розірвання договору позивач вимагає стягнення збитків), то ті самі документи, які раніше не були належними, можуть набути вирішального значення. Отже, належність безпосередньо впливає на досягнення стандарту доказування, оскільки саме вона визначає, які докази враховують під час оцінки їх достатності.

Характер взаємозв'язку допустимості й належності зі стандартами доказування залежить від виду судочинства.

У кримінальному процесі, де діє стандарт «поза розумним сумнівом», будь-яка прогалина в належності чи допустимості може стати вирішальною. Недостатньо лише мати об'єктивні дані про причетність особи – вони повинні

бути отримані законним шляхом і стосуватися безпосередньо обставин, що підлягають доказуванню. Інакше ризик засудження невинного стане надто високим.

У цивільному процесі стандарт «переваги доказів» допускає більшу гнучкість. Проте й тут належність і допустимість залишаються ключовими: саме вони окреслюють межі, у яких суд порівнює імовірність різних версій. Використання неналежних доказів призвело б до викривлення балансу й порушення принципу змагальності, а застосування недопустимих – до підриву довіри до правосуддя.

В адміністративному судочинстві, де стандарти часто тяжіють до презумпції на користь громадянина, недопустимі докази, зібрані органами влади, втрачають будь-яку доказову силу. Це вкрай важливо, адже саме тут процесуальні гарантії мають урівноважити асиметрію між державою та приватною особою.

У науковому дискурсі неодноразово зауважували, що вимоги належності й допустимості інколи вступають у суперечність із завданням встановлення матеріальної істини. Суд може «бачити» істину, але не мати можливості покласти її в основу рішення через порушення процесуальних правил або через нерелевантність доказів.

На практиці взаємодія цих категорій породжує низку проблем. Судова практика фіксує випадки, коли сторони намагаються обґрунтувати позицію матеріалами, які формально відповідають вимогам допустимості, але не є належними. У таких ситуаціях досягнення стандарту доказування стає неможливим, оскільки переконливість не може ґрунтуватися на інформації, що не має відношення до предмета спору.

Інший блок проблем пов’язаний із ситуаціями, коли докази визнають недопустимими через процесуальні порушення, хоча фактично вони здатні переконати в правдивості певної обставини. Тут виявляється напруження між цінністю істини та цінністю справедливості процедури. У демократичному

правопорядку перевагу надають саме останній, адже відступ від принципу допустимості підриває легітимність судового рішення.

Слід також акцентувати на динамічності стандартів доказування. У практиці Європейського суду з прав людини спостерігається тенденція до гнучкого застосування критеріїв переконливості залежно від контексту справи. Це актуалізує від національних судів постійного узгодження стандартів із наявною системою правил допустимості та належності.

Сучасна наука пропонує різні моделі інтеграції категорій допустимості, належності й стандартів доказування. Одні автори вбачають у них самостійні елементи доказового права, які лише функціонально перетинаються. Інші ж пропонують розглядати допустимість і належність як складові ширшої категорії доказової достатності, безпосередньо пов’язаної зі стандартами.

Продуктивним видається підхід, який визнає відносну автономію цих понять, водночас зосереджує увагу на їхньому функціональному взаємозв’язку. Допустимість і належність створюють процесуальне та матеріальне підґрунтя для оцінки доказів, натомість стандарти визначають кінцевий орієнтир цієї оцінки. Така модель надає можливість гармонізувати практику й забезпечити баланс між формою і змістом правосуддя.

На підставі результатів здійсненого дослідження встановлено, що належність і допустимість доказів є вихідними критеріями їх процесуальної цінності, водночас передумовою для визнання доказів достатніми. Лише в поєднанні вони забезпечують можливість формування переконливої доказової бази, здатної відповідати вимогам різних стандартів доказування.

Достатність доказів є системною властивістю, яка поєднує якісні (достовірність, належність, допустимість) і кількісні характеристики доказового матеріалу. Вона набуває конкретного змісту залежно від стандарту доказування, що застосовують на певній стадії кримінального провадження:

– «обґрунтована підозра» – мінімальний рівень переконливості, необхідний для початку кримінального переслідування;

– «достатня підстава» – проміжний рівень, що зумовлює можливість прийняття процесуальних рішень;

– «поза розумним сумнівом» – найвищий стандарт, без досягнення якого постановлення обвинувального вироку є неможливим.

Аналіз наукових підходів дає підстави стверджувати, що стандарти доказування поєднують як об’єктивний, так і суб’єктивний критерії: з одного боку, вони закріплені в кримінальному процесуальному законодавстві й судовій практиці, з іншого – відображають рівень внутрішнього переконання суб’єкта доказування.

Висновки до розділу 2

1. Встановлено, що електронні докази охоплюють широкий спектр інформації – від файлів і листувань у месенджерах до записів камер спостереження й даних із хмарних сховищ. Їх належність у кримінальному провадженні зумовлена зв’язком із предметом доказування, що потребує ретельної ідентифікації користувача, джерела походження та часових меж. Розглянуто питання автентичності, зокрема доведено, що цифровий доказ слід вважати належним лише тоді, коли його можна об’єктивно пов’язати з подією, особою чи обставиною, які досліджують. Визначено «мінімальний стандарт» належності електронних доказів, що передбачає: ідентифікацію цифрових даних (зв’язок із користувачем/пристроєм/акаунтом), їх локалізацію (місце/сховище/сервіс), прив’язку в часі (timestamp/метадані) та відтворення (можливість отримати перевірну копію).

2. Констатовано, що допустимість електронних доказів залежить від суворого дотримання процесуальних вимог щодо їх отримання, фіксації та зберігання. З’ясовано, що судова практика під час вирішення питання про належність і допустимість електронних доказів встановлює: законність доступу/вилучення електронних документів, наявність підтвердження

автентичності (електронний підпис, сертифікат, висновок експерта, хеш-суми) забезпечення рівності сторін (можливість огляду копії або оригіналу стороною захисту). У цьому контексті зазначено, що порушення порядку вилучення чи копіювання даних, відсутність судового дозволу на доступ або технічні помилки під час обробки носіїв неминуче призводять до ризику визнання доказу недопустимим. Водночас на практиці законодавець поступово формує підхід, орієнтований на мінімізацію вилучення обладнання та акцент на копіюванні інформації, що сприяє запобіганню зловживанням і забезпеченню балансу між інтересами слідства та правами власників техніки.

3. Акцентовано на важливості дотримання принципу «ланцюга збереження доказів» (chain of custody), відповідно до якого кожен етап роботи з електронними даними – виявлення, копіювання, зберігання та передача – має бути задокументовано й перевірено. Зазначено, що використання технічних методів підтвердження автентичності (електронні підписи, контрольні хеш-суми, форензичні образи) створює підґрунтя для визнання доказів достовірними й виключає можливість їх непомітної модифікації. Брак зазначеного технічного підтвердження спричиняє ускладнення судової оцінки цифрових доказів.

4. Запропоновано на законодавчому рівні закріпити визначення електронного (цифрового) доказу як самостійного джерела з відповідними правилами поводження з ним шляхом внесення змін до ст. 84 КПК України. Обґрунтовано необхідність розроблення підзаконних нормативних актів або офіційних методичних рекомендацій для слідчих і судів щодо роботи із цифровими доказами, які встановлюватимуть стандарти фіксації та зберігання електронних даних. Аргументовано доцільність підвищення рівня технічної оснащеності та кваліфікації правоохоронних органів у галузі комп’ютерної криміналістики, щоб забезпечити належну реалізацію нових норм на практиці.

5. Виокремлено специфічні риси електронних доказів у контексті їх допустимості в кримінальному провадженні: 1) фізичне існування електронного документа неможливе поза межами носія інформації, тому для

забезпечення достовірності доказу необхідно ідентифікувати носій, ураховуючи його тип, модель й індивідуальні машинні характеристики; 2) мають нематеріальний характер, що унеможливлює їх безпосереднє сприйняття без застосування відповідних програмно-технічних засобів і спеціального інструментарію; 3) можуть бути змінені, пошкоджені або знищені в процесі експлуатації пристрою користувачем чи під впливом фізичних чинників; 4) за стадіями виготовлення документи, зокрема електронні, поділяють на оригінали, дублікати, копії та виписки, а позначення «оригінал», «дублікат», «копія» є умовними, тому що в усіх цих випадках електронний документ залишається оригіналом.

6. Визначено основні засади під час роботи з електронними доказами: 1) законність, що передбачає вивчення доказів в електронній формі, дотримання чинного законодавства та загальних процесуальних і криміналістичних принципів; 2) цілісність даних, що виключає матеріальні зміни інформації, електронних пристроїв чи носіїв інформації, що має доказове значення; 3) документування будь-яких дій щодо електронних доказів, зберігання таких документів на випадок перевірки, щоб незалежна третя сторона мала можливість повторити ці дії та одержати аналогічний результат; 4) залучення спеціалістів під час огляду (обшуку), якщо є ймовірність виявлення електронних доказів; 5) наявність відповідної фахової підготовки слідчого, дізнавача, прокурора, що необхідна в разі відсутності спеціалістів у сфері електронних доказів; 6) розумна обережність, що передбачає уникнення будь-яких навмисних або ненавмисних дій, що можуть призвести до пошкодження потенційних доказів, представлених у цифровій формі.

7. Окреслено специфіку критеріїв допустимості електронних доказів: 1) належне джерело отримання доказів; 2) належний суб’єкт; 3) належний спосіб збирання доказів. У контексті зазначеного увагу зосереджено на останньому критерії. На підставі аналізу положень ст. 93 КПК України виокремлено такі законні способи збирання електронних доказів стороною

обвинувачення: надання доказів добровільно учасником кримінального провадження (отримання); витребування доказів; проведення тимчасового доступу до електронного документа (як заходу забезпечення); проведення слідчих (розшукових) дій (огляд, обшук); проведення негласних слідчих (розшукових) дій. Натомість сторона захисту, потерпілий та його представник можуть збирати електронні документи шляхом: 1) одержання чи витребування їх від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, службових і фізичних осіб; 2) ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій стороною обвинувачення. Зазначено, що в разі реалізації права сторони захисту, потерпілого на ініціювання проведення процесуальних дій учасники є лише ініціаторами, а суб'єктами збирання в разі задоволення клопотання буде слідчий, дізнавач або прокурор.

8. У контексті дослідження питання допустимості й належності електронних доказів окреслено зміст стандартів доказування, які у фаховій літературі диференційовано залежно від стадії кримінального провадження: «обґрунтована підозра» (мінімальний рівень переконливості, необхідний для початку кримінального переслідування); «достатня підстава» (проміжний рівень, що зумовлює можливість прийняття процесуальних рішень); «поза розумним сумнівом» (найвищий стандарт, без досягнення якого постановлення обвинувального вироку є неможливим).

РОЗДІЛ 3
ПОРЯДОК ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ ТА СУДОВОГО ПРОВАДЖЕННЯ

3.1. Вилучення та процесуальне оформлення електронних доказів під час проведення досудового розслідування

Активне впровадження цифрових технологій у повсякденне життя зумовило стрімке збільшення кількості електронних даних, що можуть бути доказами під час здійснення досудового розслідування та судового розгляду. Електронні листування, записи з камер спостереження, дані мобільних телефонів, інформація з мережі Інтернет та інших цифрових носіїв нині нерідко містять відомості про обставини вчинення відповідних протиправних діянь. У цих умовах перед правоохоронними органами постає важливе завдання – належно виявити, вилучити й зафіксувати електронні докази, щоб зберегти їхні достовірність і допустимість у суді. Проблема полягає в тому, що традиційні процесуальні підходи, розраховані переважно на речові докази й документи в паперовій формі, не цілком ураховували специфіку цифрових даних. Брак до недавнього часу детальних інструкцій щодо роботи з електронними носіями інформації призводив до різної інтерпретації на практиці та ризику втрати або пошкодження важливих даних. Отже, актуальним є дослідження правових і криміналістичних аспектів вилучення електронних доказів й оформлення результатів таких дій у матеріалах досудового розслідування.

Питання використання електронних доказів у кримінальному процесі привертає увагу науковців і практиків. Зокрема, різні аспекти отримання, дослідження та оцінки цифрових доказів розглядали у своїх працях А. М. Ангеленюк [2], А. М. Гаркуша [40]; В. В. Мурадов [64], І. Г. Каланча

[37; 38; 39], О. В. Сіренко [93], А. В. Скрипник [94], А. В. Столітній [100] та інші дослідники. Низку сучасних робіт присвячено як теоретичним засадам правової природи електронних доказів, так й аналізу судової практики щодо їх допустимості. Слід виокремити дослідження іноземного досвіду: Н. М. Сенченко та В. Ю. Чумаченко проаналізували законодавче регулювання електронних доказів у ЄС, США, Великій Британії, Китаї, що надає можливість урахувати найкращі практики.

Кримінальне процесуальне законодавство України закріплює базові положення щодо електронних доказів, хоча їхній статус протягом тривалого часу залишався нечітким. Згідно з ч. 1 ст. 99 КПК України, документом є матеріальний об'єкт, що містить зафіксовані відомості, які можуть бути доказами в кримінальному провадженні. Матеріали фото-, відеозйомки, звукозапису й інші носії інформації, зокрема комп'ютерні дані, віднесені законом до документів (ч. 2 ст. 99 КПК). Отже, електронні докази за чинним підходом законодавця розглядають як різновид документів у кримінальному процесі. Водночас фізичні носії, на яких зберігають ці дані (комп'ютери, смартфони, накопичувачі тощо), можуть бути визнані речовими доказами за змістом ст. 98 КПК, оскільки є матеріальними об'єктами, пов'язаними з подією злочину [58].

Поняття «електронний доказ» безпосередньо не визначено в КПК, але розроблене практикою та доктриною на основі законодавства про електронні документи. Згідно з положенням Закону України «Про електронні документи та електронний документообіг», електронний документ не можна визнати недопустимим доказом лише через його форму (ч. 2 ст. 8 цього Закону). Якщо електронний документ існує на кількох носіях, кожен примірник вважають оригіналом (ст. 7 цього Закону). Це означає, що однакові за змістом копії файлу на різних носіях визнають рівноцінними оригіналами. У практичному вимірі це надзвичайно важливо: наприклад, копія файлу на сервері та його копія на вилученому жорсткому диску є оригіналами документа, якщо їх автентичність підтверджено.

За своєю сутністю електронний доказ – це інформація про факти в цифровій формі. Суддя Верховного Суду Н. Марчук зауважила, що до електронних доказів належать: файли з текстовими документами, графічними зображеннями; файли з фото- та відеоматеріалами, аудіозаписами (зокрема записаними на мобільний телефон); електронні файли – додатки до протоколів слідчих дій (наприклад, відеозапис слідчого експерименту на диску); вебсайти (вміст інтернет-сторінок); дані месенджерів (чат-листування в Skype, Viber, Telegram, Facebook тощо); відео з камер спостереження; скриншоти (цифрові знімки екрана) й інші схожі об'єкти [58]. Цей перелік ілюструє широкий діапазон цифрових слідів, які можуть бути доказами. Спільною рисою є те, що вони не існують у паперовому вигляді, а отже, потребують спеціального підходу до збирання та фіксації.

Національний законодавець поступово вдосконалює правові норми, щоб адаптувати їх до реалій цифрової ери. 2017 року до процесуальних кодексів (цивільного, господарського, адміністративного) було введено поняття «електронні докази» як окремого засобу доказування [88]. У кримінальному процесі аналогічні зрушення відбулися пізніше. Важливим кроком стало ухвалення Закону України від 15 березня 2022 року № 2137-IX, яким внесено зміни до КПК та Закону України «Про електронні комунікації» з метою підвищення ефективності досудового розслідування, зокрема «за гарячими слідами» та протидії кіберзлочинності. Цим актом було суттєво покращено правове регулювання процесу доказування з використанням електронних доказів [88]. Зокрема, уточнено процедури отримання інформації з електронних систем та розширено можливості слідчих у цій сфері.

Статтю 99 КПК України доповнено положенням, згідно з яким копії інформації (зокрема комп'ютерних даних), отримані слідчим або прокурором із залученням спеціаліста, суд визнає як оригінал документа. Це надзвичайно важлива норма, яка фактично легалізує застосування криміналістичних методів копіювання цифрових даних. Вона означає, що якщо слідчий за участю спеціаліста з інформаційних технологій скопіює потрібні файли з

комп’ютера чи іншої електронної системи на окремий носій, така копія матиме таку саму доказову силу, що й початковий носій інформації. Тож немає потреби завжди вилучати фізичний носій (наприклад, сервер або мобільний телефон) для подання доказу до суду – достатньою є належно виготовлена копія. Закон водночас акцентує, що створення копії має відбуватися із залученням спеціаліста, що гарантує правильність процедури. Ця новація спрямована на баланс між ефективністю розслідування та правом власників на користування технікою: оригінальні пристрої пропонують вилучати лише за необхідності.

Попри позитивні зрушення, низка аспектів досі потребує врегулювання. Експерти констатують брак детального порядку вилучення електронних доказів: коли саме слід вилучати оригінальні електронні носії, у якій формі долучати цифрові дані до матеріалів справи, як їх зберігати та хто відповідальний за цілісність цих даних. У згадуваному Законі 2022 року ці питання порушено, але не вичерпано. Представники правничої спільноти пропонували прямо передбачити, що оригінали електронних доказів вилучають лише у виключних випадках, а також установити детальну процедуру їх долучення, реєстрації та зберігання в матеріалах провадження з визначенням кола відповідальних осіб. На момент написання дослідження спеціалізованої інструкції чи підзаконного акта, який регламентував би покроково дії слідчого в процесі роботі з електронними доказами, в Україні ще не затверджено. Тому практичні навички ґрунтуються на напрацюваннях криміналістики й закордонних рекомендаціях.

У цьому контексті слід зауважити, що абсолютна більшість опитаних (100 %) засвідчила необхідність законодавчого закріплення процесуального порядку вилучення, копіювання та отримання електронних (цифрових) даних шляхом складання протоколу із зазначенням способу отримання, технічних засобів і хеш-значень файлів.

У кримінальному процесі є кілька процесуальних механізмів для отримання електронної інформації в розпорядження слідства.

Найпоширенішим із них є обшук (ст. 234 КПК), у межах якого можуть бути вилучені комп'ютери, телефони, носії пам'яті й інші пристрої, що містять дані, які мають значення для справи. У протоколі обшуку обов'язково фіксують виявлені й вилучені електронні носії з детальним описом (тип пристрою, модель, серійний номер тощо). Інший інструмент – тимчасовий доступ до речей і документів (ст. 160 КПК України): слідчий суддя може винести ухвалу, яка зобов'язує певну особу або установу надати інформацію, зокрема в електронній формі. Це застосовують, наприклад, для отримання даних від інтернет-провайдерів, мобільних операторів, хмарних сервісів або із серверів компаній. У такому разі носії інформації можуть і не вилучати фізично – здійснюють копіювання файлів або витяг записів з баз даних за участю відповідальних осіб. Також КПК передбачає можливість тимчасового вилучення майна (ст. 167 КПК) – фактичного вилучення об'єкта без ухвали суду в невідкладних випадках, з подальшим отриманням дозволу суду. Тимчасове вилучення може стосуватися й електронних пристроїв, якщо їх виявлено, наприклад, під час затримання особи або огляду місця події, і є ризик, що зволікання призведе до втрати даних.

Електронні докази мають вразливу природу: їх можна легко скопіювати, змінити або знищити без фізичних слідів. Тому надзвичайно важливо під час вилучення дотриматися таких умов, щоб інформація залишилася в тому самому вигляді, як і на момент виявлення. Міжнародні стандарти цифрової криміналістики сформулювали базові принципи поводження з електронними доказами. У Великій Британії діють Принципи ACPO (Association of Chief Police Officers) для цифрових доказів, які, зокрема, проголошують: жодна дія, вчинена правоохоронцями щодо електронного пристрою, не повинна змінювати дані, які потім використовуватимуть у суді [125]. Якщо необхідно отримати доступ до оригінальних даних, особа, що це робить, повинна мати відповідну компетентність і бути здатною пояснити суду свої дії та їх наслідки [125]. Обов'язково ведуть детальний журнал (аудит-трейл) усіх дій із цифровими носіями, щоб сторонній експерт міг перевірити процедуру й

отримати ті самі результати. Ці принципи спрямовані на збереження цілісності й достовірності електронних доказів.

На практиці дотримання таких вимог означає, що під час вилучення цифрового носія слід: 1) унеможливити зміну даних на ньому після вилучення (наприклад, вимкнути живлення комп'ютера правильно, використати спеціальні блокувальні пристрої для портів, помістити смартфон в екранований контейнер для блокування сигналів тощо); 2) зафіксувати всі дії – час вилучення, хто мав доступ, серійні номери техніки, стан пристрою (ввімкнений чи вимкнений), наявність запаролення або шифрування тощо; 3) якнайшвидше здійснити дублювання даних (створення копії) у присутності понятих або під відеофіксацію, із залученням ІТ-спеціаліста. Під час копіювання рекомендують застосовувати криптографічні хеш-алгоритми (наприклад SHA-256) для обчислення контрольних сум файлів чи носія загалом до і після копіювання. Збіг хеш-суми підтвердить, що копія та оригінал ідентичні, а жодних змін не відбулося. Такий підхід вже застосовують українські експерти: уповноважена особа або призначений експерт може провести спеціальне дослідження для встановлення автентичності електронних даних, зокрема визначити контрольну суму файлу чи каталогу файлів.

Результати вилучення електронних доказів має бути ретельно задокументовано в процесуальних актах. Якщо дані отримано під час обшуку – складають протокол обшуку (ст. 104, 236 КПК), де зазначають, які саме електронні пристрої чи носії вилучено, їх опис й обставини виявлення. У протоколі доцільно фіксувати й технічні особливості: наприклад, «вилучено системний блок комп'ютера Accer, серійний №...; під час вилучення комп'ютер знаходився у ввімкненому стані, робота припинена шляхом натискання кнопки вимкнення; жорсткий диск вилучено окремо, пломба №...». Якщо проводили копіювання на місці, його можна оформити як додаток до протоколу або окремий акт за участю спеціаліста. У випадку тимчасового доступу до речей, коли надають копії електронних даних, особа, що їх видає

(скажімо, представник компанії), складає здебільшого супровідний лист або акт, де підтверджує, що надана інформація відповідає оригіналу. У будь-якому разі важливо простежити ланцюжок зберігання доказу: хто і коли отримав носій, де його зберігали, хто мав до нього доступ. Для цього слідчий здійснює відповідні записи в журналі речових доказів, опечатує носії та здає їх до камери схову речових доказів або на експертизу.

Кримінальний процесуальний кодекс України (ст. 99) дозволяє слідству використовувати копії електронної інформації на рівні з оригіналами, за умови дотримання процедури їх створення. На практиці це реалізують так: після вилучення пристрою слідчий призначає комп'ютерно-технічну експертизу або залучає спеціаліста для витягання даних. Спеціаліст створює цифрову копію (наприклад, образ жорсткого диска або дамп пам'яті телефона) і записує її на окремий носій (DVD, флешпам'ять, зовнішній диск). Такий носій опечатують і долучають до справи як матеріальний носій інформації – як речовий доказ, що містить документальні електронні дані. Одночасно експерт або слідчий може зробити роздруківку або скриншоти найбільш значущих файлів (наприклад, листування з месенджера, окремі фото, фрагмент відео) для зручності огляду в суді. Паперова копія електронного доказу не є власне електронним доказом – це лише засіб наочності. Її слід засвідчувати належно. У кримінальному провадженні паперові копії електронних даних можуть бути додані до матеріалів, але суд вимагає, щоб сторона, яка подає доказ, забезпечила можливість перевірити його автентичність на оригінальному електронному носії або на копії, прирівняній до оригіналу.

Якщо сторона обвинувачення подає лише роздруківку (наприклад, чат з телефону) без власне файлу чи носія, захист може ставити під сумнів допустимість такого доказу – і суди нерідко стають на бік захисту. Наприклад, були випадки, коли паперову копію електронного документа суд не врахував через неподання оригіналу або належно посвідченої електронної копії. Касаційний кримінальний суд Верховного Суду протягом 2020–2021 років неодноразово зауважував, що якщо електронні дані (аудіо, відео тощо) подані

на розгляд суду лише у вигляді паперового додатка (транскрипту, скриншоту) і не підтверджені оригінальним носієм або офіційно виготовленою копією, то такі докази можуть бути визнані недопустимими [88]. Отже, процесуальне оформлення електронного доказу має завершуватися тим, що в матеріалах справи наявний або електронний носій (оригінал чи копія), або документ, який однозначно підтверджує його зміст й автентичність (наприклад, висновок експерта, що описує знайдені файли, із хеш-значеннями).

Після вилучення та фіксації доказів постає питання їх дослідження в межах досудового розслідування. Слідчий має право провести огляд речового доказу чи документа (ст. 237 КПК), зокрема, оглянути вміст електронного пристрою. Проте на практиці слідчі зрідка самостійно переглядають інформацію на складних цифрових носіях через брак технічних знань і ризик зіпсувати дані. Частіше призначають експертизу: експерт у лабораторії копіює дані, відновлює видалені файли, знімає захист тощо, а результати подає у висновку експерта. Такий висновок є процесуальним документом (джерелом доказів), у якому експерт може вказати, які конкретно файли виявлено (зазначити їх зміст, назви, дати модифікації тощо), а також носій, з якого їх отримано. Висновок експерта долучають до матеріалів і розглядають у сукупності з іншими доказами.

Вилучені оригінальні пристрої зберігають переважно серед речових доказів (у спеціальних приміщеннях при органі досудового розслідування або суді). З огляду на їхні особливості, слід вживати заходів для запобігання деградації носіїв (магнітні диски, флешпам’ять можуть з плином часу пошкоджуватися, також небезпеку становлять електромагнітне випромінювання, волога, екстремальні температури). Копії на цифрових носіях теж слід зберігати належно опечатаними. Важливим аспектом є конфіденційність: електронні докази можуть містити приватні дані сторонніх осіб, тому доступ до них мають лише уповноважені учасники провадження. У зв’язку з цим законодавство обмежує коло осіб, яким можна надавати

тимчасовий доступ до інформації, отриманої під час слідства, і покладає відповідальність за нерозголошення на слідчого, прокурора, експерта.

Аналіз судової практики засвідчує, що головним критерієм оцінки електронного доказу є дотримання встановленого порядку його отримання. Порушення процедури прямо веде до визнання доказу недопустимим, навіть якщо його зміст викриває обвинуваченого. Касаційний кримінальний суд неодноразово акцентував, що нова природа носія не звільняє сторону від обов'язку суворо виконувати процесуальні вимоги. Класичним прикладом недопустимості є отримання відеозапису оперативним шляхом до внесення відомостей в ЄРДР. Тобто, коли ще не було почато офіційне провадження, а оперативні працівники «на випередження» здобули запис, суд не бере його до уваги як доказ, бо його здобуто поза межами процесу. Інший приклад: якщо слідчий просто переглянув відео і склав протокол огляду, але не оформив належно вилучення носія, суд може відхилити такий протокол через порушення порядку отримання доказу.

Проблеми постають і в ситуаціях, коли не забезпечено надання оригіналу або належної копії. В одній зі справ захист клопотав визнати недопустимим протокол слідчого експерименту, оскільки немає оригінального носія з відеозаписом цього експерименту – суд погодився, що без носія автентичність відео не підтверджено. Аналогічно аудіозаписи розмов, здійснені без відповідної ухвали та без носія, що їх містив, були виключені з доказів. Отже, для сторони обвинувачення важливо заздалегідь подбати, щоб усі цифрові докази були здобуті законним шляхом і документально підтверджені.

Слід зауважити, що судова практика в питаннях електронних доказів ще формується і не завжди є одноманітною [88]. Деякі суди першої інстанції можуть механічно відмовлятися приймати, скажімо, роздруківки SMS, інші – приймають їх, якщо сумнівів у достовірності немає. Однак загальна тенденція на вищому рівні така, що сторона, яка подає електронний доказ, несе тягар доведення його достовірності й належного джерела походження. У цьому

сенсі електронний доказ прирівнюють до звичайного документа: потрібно продемонструвати без розумного сумніву, що інформація така сама, яку було отримано спочатку [125]. Для цього й застосовують усі зазначені вище методи: залучення фахівців, протоколи, хеш-суми, експертні висновки.

Практика інших країн демонструє схожі виклики у сфері цифрових доказів і пропонує шляхи їх вирішення. Уже згадуваний британський підхід (принципи ACPO) акцентує на технічній стороні збереження даних. У США розроблено детальні інструкції для «першого реагування» на місці вилучення електроніки (First Responder Guides), які регламентують навіть дрібниці: від того, як фотографувати екран ввімкненого комп'ютера – до порядку вилучення інформації із «хмари» через провайдера. У Європейському Союзі протягом останніх років посилену увагу спрямовано на транскордонне отримання електронних доказів. Через брак єдиного підходу в різних країнах і складність співпраці ЄС 2023 року ухвалив два регламенти (№ 2023/1543 та № 2023/1544), спрямовані на уніфікацію порядку отримання електронних доказів за запитами між державами [88]. У цих актах запроваджено механізми «європейського ордера на надання електронних доказів», що дає змогу компетентним органам однієї країни оперативно отримувати дані від провайдерів, що перебувають в іншій країні ЄС. Одночасно акцентують на необхідності балансу між ефективністю розслідування та захистом права на приватність [88]. Для України, яка обрала курс на євроінтеграцію, важливо враховувати ці тенденції: адаптацію національного законодавства про електронні докази до європейських стандартів посилить можливості правоохоронців і сприятиме взаємному визнанню доказів.

Крім того, міжнародні організації розробляють рекомендації щодо роботи із цифровими доказами. Наприклад, рекомендації Ради Європи і Європолу містять поради щодо виокремлення релевантної інформації за великих обсягів даних, забезпечення прозорості експертиз і використання спеціалізованого програмного забезпечення для аналізу даних. У деяких країнах (США, Канада, Австралія) діють стандарти ліцензування цифрових

експертів, що гарантує їхню компетентність під час участі в слідчих діях. Отже, загальний висновок із закордонного досвіду такий: успішне використання електронних доказів потребує чіткого регламенту на рівні закону й відомчих інструкцій, технічної грамотності слідчих та експертів, а також міжнародної співпраці, оскільки цифрові сліди часто виходять за межі однієї держави.

2023 року в ЄС запрацювали Regulation (EU) 2023/1543 та Directive (EU) 2023/1544, які в аналітиці 2024–2025 років описують як перехід до моделі прямих розпоряджень постачальникам послуг – European Production Orders (EPOC) та European Preservation Orders (EPOC-PR). Ці інструменти дають змогу виходити за межі повільних класичних процедур взаємодопомоги, забезпечуючи швидке вилучення або збереження даних, водночас встановлюють формалізовану електронну форму відповіді, яку прирівнюють до паперової, її не може відхилити національний орган лише з мотивів відсутності паперової копії [128, с. 12–13]. Процедурні строки структуровано чітко: базовий строк виконання становить десять днів, а для невідкладних випадків – вісім годин; для недобросовісних провайдерів передбачено штрафи до двох відсотків річного світового обороту, що формує реальні стимули до співпраці та дисциплінує ринок електронних комунікацій [151, с. 8–9]. Доктрина акцентує, що така архітектура змінює парадигму від державоцентричної взаємодопомоги до прямого правового зв’язку між органом правосуддя та провайдером у межах ЄС, але фільтрує цей зв’язок через гарантії прав особи, привілеї та імунітети, а також вимоги до обробки персональних даних, зокрема у контексті GDPR [128, с. 12–13; 150, с. 259–262]. Для української практики це означає необхідність раннього ініціювання preservation через партнерські канали, технічної синхронізації формулярів і мови сертифікатів, використання захищених каналів обміну та негайного формування ланцюжка цілісності із фіксацією метаданих, часу передачі й контрольних сум, аби надалі безперешкодно долучити ці матеріали до кримінального провадження як документи в розумінні ст. 99 КПК.

Під час роботи із хмарними і транскордонними даними слідчий має послідовно проходити декілька змістових етапів, які уникають формальної списковості, але вимагають матеріалізації в процесуальних актах. Насамперед ідентифікують провайдер і релевантну юрисдикцію, від чого залежить вибір інструмента взаємодії – чи то запит у межах взаємного визнання і співпраці в ЄС, чи традиційні канали міжнародної правової допомоги; одночасно, не зволікаючи, ініціюють збереження чутливих даних, оскільки політики retention у провайдерів жорстко обмежують тривалість їхнього існування [151, с. 8–9]. Далі предметний опис запитуваної інформації має бути вузьким, із зазначенням ідентифікаторів облікових записів, часових інтервалів і типів даних, а мовні параметри документів погоджують із прийнятною для провайдера мовою сертифікатів [128, с. 12]. Отримання відбувається через передбачені регламентом захищені ІТ-системи, що забезпечують передачу електронних документів із юридичною силою паперових [128, с. 12–13; 132; 149]. Безпосередньо після одержання даних здійснюють хешування відповідних наборів, складають акт приймання з переліком файлів і метаданих та відомостями про версії формулярів; ці носії долучають як речові докази, натомість дані, з огляду на кваліфікацію ст. 99 КПК, набувають статусу документів. За потреби призначають комп’ютерно-технічну експертизу із завданням підтвердити автентичність і відтворюваність, а на стадії відкриття матеріалів стороні захисту забезпечують доступ саме до електронної форми з відповідними хеш-ідентифікаторами, оскільки подання лише роздруківок або скриншотів істотно підвищує ризик заперечень допустимості, що підтверджує й узагальнення практики [41, с. 1001–1003].

Можна виокремити дві стійкі зони процесуального ризику для електронних доказів. Перша стосується втрати доказової сили паперових відтворень цифрового змісту, коли суд позбавлений можливості співвіднести такі аркуші з оригінальним електронним джерелом або прирівняною до оригіналу копією та перевірити їхню цілісність на рівні контрольних сум, часових позначок і метаданих; саме тому акцентовано на обов’язковості

надання електронного носія або верифікованої копії разом з експертним підтвердженням способу їх одержання та незмінності [41, с. 1001–1003]. Друга зона стосується поширеного на практиці «оперативного» отримання відео- й аудіозаписів до внесення відомостей у ЄРДР, що згодом провокує визнання таких матеріалів недопустимими, з огляду на позапроцесуальний спосіб їх здобуття; узагальнення засвідчують, що саме ці порушення найчастіше призводять до виключення цифрових матеріалів із доказової бази, незалежно від їхнього змісту [41, с. 1001–1003]. На цьому тлі європейська доктрина вбачає в пакеті e-Evidence не лише механізм пришвидшення доступу, а й інструмент стандартизації ланцюжка походження та електронної форми відповіді, що спрощує судову оцінку в державах-членах і, за умови належного документування міжнародної взаємодії, полегшує інтеграцію таких доказів у національні провадження третіх країн [150, с. 259–262; 151, с. 1–2, 8].

Практичні наслідки для України виявляються в трьох пов’язаних площинах. По-перше, планування дій слідчого має одразу враховувати політики збереження в провайдерів і прив’язувати ініціювання preservation до якомога ранішого можливого моменту, інакше «хмарна» частина доказового масиву буде безповоротно втрачена до завершення локальних слідчих дій [88, с. 8–9]. По-друге, процесуальні акти потребують уніфікування: доцільно застосовувати стандартизований додаток до протоколу, який фіксує канал і сертифікат, перелік файлів і метаданих, контрольні суми, посадові дані учасників та часову розмітку операцій; така уніфікація підвищує відтворюваність і прозорість ланцюжка володіння. По-третє, експертиза має бути зорієнтована не лише на зміст, а передусім на походження і цілісність, тобто на відтворення того самого набору бітів із тим самим хеш-ідентифікатором, що кореспондує з підходами ЄС до рівності електронних і паперових форм доказів [128, с. 12–13; 132]. Узгодження цих кроків із судовою практикою, яка вимагає підтверджуваного джерела походження та можливості верифікації електронного доказу, створює внутрішньо несуперечливу модель

допустимості, що витримує як національну перевірку, так і перевірку на рівні співпраці з органами держав – членів ЄС.

Електронні докази стали невіддільною частиною сучасного кримінального провадження, що ставить нові вимоги до діяльності органів досудового розслідування. Здійснений аналіз дає підстави для таких висновків. По-перше, електронні докази в Україні юридично прирівняні до документів, а їхні матеріальні носії – до речових доказів. Законодавство (ст. 99 КПК) наразі передбачає можливість використання копій цифрової інформації як оригіналів за умови правильного виготовлення таких копій із залученням спеціаліста. Це прогресивна норма, що узгоджується з практичними потребами: вона дає змогу мінімізувати вилучення техніки й водночас зберегти доказову інформацію. По-друге, процесуальне оформлення електронних доказів потребує особливої ретельності: обов'язкове документування кожного етапу (вилучення носія, копіювання, дослідження), засвідчення автентичності даних (через хеш-суми, експертні висновки) і забезпечення доступу до «оригіналу» у разі потреби суду. Недотримання цих вимог безпосередньо загрожує втратою доказової сили матеріалів – суди обґрунтовано визнають недопустимими цифрові докази, здобуті з порушенням процедури або належно не підтверджені.

По-третє, нагальною є потреба в подальшому вдосконаленні правового регулювання та розробленні підзаконних актів, що детально регламентують поводження з електронними доказами. Зокрема, доцільно розробити офіційну інструкцію або методичні рекомендації для слідчих і прокурорів щодо вилучення цифрових носіїв, копіювання інформації, використання спеціальних технічних засобів і зберігання електронних речових доказів. У цій інструкції слід визначити, що фізичні носії вилучають лише у випадках, коли без цього неможливо забезпечити збереження даних або коли носій має самостійну доказову цінність. Необхідно також установити процедури залучення ІТ-спеціалістів на місці події, оформлення результатів їхньої роботи

(складання актів, звітів тощо) і порядок передачі електронних доказів на експертизу й до суду.

По-четверте, важливим напрямом є підготовка кадрів: підвищення кваліфікації слідчих у галузі цифрової криміналістики, забезпечення підрозділів кіберполіції сучасними засобами для вилучення та аналізу даних, створення спільних команд слідчих й ІТ-фахівців для розслідування кіберзлочинів. Без належного розуміння технічних нюансів навіть досконалі норми можуть лишитися лише номінальними.

Узагальнюючи іноземний досвід, можна рекомендувати активніше впроваджувати міжнародні стандарти роботи з електронними доказами. Принципи забезпечення цілісності й автентичності цифрових даних універсальні: незмінність даних з моменту вилучення до подання суду, компетентність осіб, що працюють з носіями, повний облік усіх дій і збереження ланцюжка володіння доказом. Дотримання цих принципів підвищить рівень довіри суду до електронних доказів і сприятиме формуванню єдиної сталої практики їх оцінки.

Отже, вилучення та процесуальне оформлення електронних доказів потребують комплексного підходу, що поєднує сучасне законодавче забезпечення, методичну базу й технічну підготовку учасників розслідування. Лише за таких умов цифрова інформація цілком реалізує свій потенціал у викритті злочинів, не породжуючи нових сумнівів стосовно достовірності й допустимості доказів.

3.2. Особливості доказування на підставі електронних доказів: судова практика

У науці кримінального процесуального права протягом тривалого часу триває дискусія серед учених щодо визначення поняття, місця та ролі електронних доказів у кримінальному провадженні. Це зумовлено не тільки

браком нормативного закріплення електронних доказів у Кримінальному процесуальному кодексі України, а й специфікою порядку їх виявлення, дослідження, вилучення, зберігання та оцінки.

Л. Мілімко вважає, що електронні докази доцільно визнати самостійною групою доказів і закріпити в КПК України. Термін «електронний доказ у кримінальному судочинстві» запропоновано тлумачити як інформацію про факти й обставини кримінального провадження, що зафіксована в електронній формі та є відмінною від доказів в електронному вигляді, одержана в передбаченому кримінальним процесуальним законодавством порядку [63, с. 302].

Унаслідок розвитку комп'ютерних технологій та їх активного застосування у середині минулого століття сформувалася концепція комп'ютерних доказів (computer evidence), які генерують електромагнітні сигнали під час роботи комп'ютерної системи, їх застосовують для встановлення елементів предмета доказування [111]. Згодом, після залучення мережевих технологій, з'явилося поняття мережевих доказів (network evidence), яке стосується електромагнітних сигналів у мережевому середовищі. Наприкінці XX ст., крім комп'ютера й мережі, з'явилася значна кількість цифрових пристроїв, призначених для передавання цифрових сигналів телефонного, телеграфного й телевізійного зв'язку. У правничих колах результати використання таких цифрових пристроїв назвали «цифровими доказами» (digital evidence) або «електронними доказами» (electronic evidence) [140, с. 112].

Терміни «цифрові докази» й «електронні докази» у спеціальній літературі й офіційних документах переважно використовують як синоніми. Технічно коректним є застосування категорії «цифрові докази» [144, с. 41]. Поняття «цифровий» позначає тип сигналу, що застосовується у пристрої, відмінний від аналогового. Цифровий сигнал є непостійним, дискретним у вигляді хвиль квадратної форми, натомість аналоговий – завжди постійний, безперервний у формі синусоїди. Пристрої працюють як з аналоговими, так і

з цифровими сигналами, проте більшість мікропроцесорів, комп'ютерів і логічних блоків є суто цифровими компонентами. Однак, незалежно від виду сигналу, його створення, передачу, збереження, застосування забезпечує відповідний електронний пристрій. Прикметник «електронний» означає створений, записаний, переданий чи збережений в цифровій або іншій нематеріальній формі за допомогою електронного, магнітного, оптичного чи будь-якого іншого способу, що має можливості для створення, запису, передачі або збереження даних. Використання слова «електронний» для позначення виду доказу не обмежує тип електроніки (цифрової, аналогової, мікроелектроніки, оптоелектроніки) чи інтегральних схем, результати використання яких можуть мати значення для кримінального провадження. Тож цифровим є електронний доказ, згенерований у числовому форматі, або перетворений у нього. Одночасно з появою нових технологій застосування цифрових доказів стрімко активізуватиметься [111].

Українське кримінальне процесуальне регулювання досі не має легальної дефініції електронних доказів. Це стосується й іноземного кримінального процесуального законодавства.

Правоохоронні органи мають ураховувати, що деякі країни не виконують запити про взаємну правову допомогу щодо злочинів невеликої тяжкості, такі обмеження встановлюють законодавство або практика. Наприклад, у США переважно не виконують запити про взаємну правову допомогу щодо злочинів, термін ув'язнення за вчинення яких становить 12 місяців і менше, або внаслідок яких була спричинена шкода на суму менше ніж 5 тис. доларів США. Отже, перш ніж направляти запит, необхідно з'ясувати в центрального органу міжнародного співробітництва конкретної держави, чи належить злочин до переліку тих, за якими здійснюють виконання запиту [7].

У разі доцільності направлення звернення про взаємну правову допомогу необхідно одержати відповідний дозвіл (ухвалу) суду. Слідчий суддя Печерського районного суду м. Києва розглянув клопотання про

тимчасовий доступ до документів, які містять охоронювану законом таємницю, що знаходяться у володінні компанії «Facebook, Inc», розташованої за адресою: м. Менло-Парк, вулиця Хакер-уей, 1, штат Каліфорнія, США (1 Hacker Way, Menlo Park, CA 94025, USA). Досудове розслідування встановило, що організована група осіб з використанням всесвітньої інформаційної системи загального доступу Інтернет вчиняють умисні дії, спрямовані на розпалювання національної, расової, релігійної ворожнечі й ненависті, приниження національної честі, гідності та образи почуттів громадян шляхом розповсюдження повідомлень у соціальних інтернет-мережах, які містять заклики до порушення рівноправності громадян залежно від їх расової, національної належності або релігійних переконань, використовуючи спеціально створені облікові записи користувачів, з метою впливу на свідомість громадян і формування заздалегідь визначеного переконання. Для встановлення події кримінального правопорушення, осіб, які здійснювали реєстрацію облікових записів і діяли за попередньою змовою з іншими співучасниками злочину для розповсюдження повідомлень у соціальних мережах, у межах слідства постала необхідність в отриманні тимчасового доступу до документів, що знаходяться у володінні компанії «Facebook, Inc» (документи щодо IP-адрес реєстрації, входу, інформації, зазначеної під час реєстрації облікових записів). Для проведення процесуальних дій на території США орган досудового розслідування, відповідно до Договору між Україною та Сполученими Штатами Америки про взаємну правову допомогу у кримінальних справах від 22 липня 1998 року, підготував запит про надання правової допомоги в кримінальному провадженні [110].

Доказам в електронній формі властиві унікальні ознаки, що відрізняють їх від інших джерел доказів і зумовлені їх природою: 1) їх творцем є як людина, так і комп’ютерна система; 2) мають нематеріальний вираз, що дає їм змогу бути збереженим на відповідному носії (смартгодиннику, смартфоні, планшеті, ноутбуку, жорстких дисках, флешнакопичувачах) чи кількох носіях

одночасно, однак без нероздільного зв'язку з ними, або перебувати у цифровому середовищі (зокрема хмарному сховищі) без такого носія; 3) унаслідок цього підлягають сприйняттю лише завдяки використанню спеціальних технічних засобів і програмного забезпечення; 4) можуть зберігатися без змін упродовж тривалого часу, бути скопійовані чи переслані, не зазнаючи коригування змісту, та не мають обмежень у кількості разів застосування; 5) з іншого боку, через свою природу докази в електронній формі піддаються маніпуляціям і знищенню; 6) копії деяких доказів в електронній формі (документів) за наявності обов'язкових реквізитів (зокрема електронного підпису) прирівнюють до оригіналу, вони можуть бути застосовані в кількох справах одночасно [63].

Важлива в питанні забезпечення єдності правозастосування позиція Верховного Суду, окреслена у справі № 751/6069/19. Відповідно до матеріалів провадження, 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 зауважив, що долучений слідчим до матеріалів провадження як речовий доказ DVD-R диск з відеозаписом обставин події було виготовлено у зв'язку з необхідністю надання інформації, яка має значення в кримінальному провадженні, є самостійним джерелом доказу, похідним від інформації, яку зберігають на комп'ютері в електронному вигляді як файли. Отже, записаний на оптичний диск – носій інформації електронний файл у вигляді відеозапису є оригіналом (відображенням) електронного документа [78].

В епоху стрімкого розвитку інформаційних технологій, активного використання електронних продуктів інформація, створена, збережена чи передана за їх допомогою, є скрізь. Доказове право й теорія доказів не можуть не відрефлексувати на такі факти.

Чимало цифрових даних не мають аналогів у вигляді доказів у позаелектронній формі. Записи смартфонів, пам'ять принтера й історія версій документів – декілька прикладів доказів в електронній формі, стосовно застосування яких у доказуванні положення традиційної теорії доказів навряд чи можуть бути повністю актуальними. Водночас не тільки процесуальна доктрина, а й правове регулювання постають перед низкою викликів, пов'язаних з особливостями такого роду доказів, а саме чутливістю до змін і знищення. Виклики ускладнюються, коли залучають такі розподілені й мережеві технології, як хмарні обчислення і технології блокчейн. Ще одну складність становить висока місткість сховищ даних, що підлягають аналізу під час кримінального провадження. Це потребує достатньої кількості технічних ресурсів. Хоча певні правові позиції ККС про застосування доказів в електронній формі сформульовано, вони досі не можуть задовольнити потреби судової практики. Тож традиційні правила кримінального процесуального доказування потребують осучаснення [111].

Водночас нормативно закріпити вичерпний перелік джерел одержання доказів в електронній формі, як це пропонують деякі дослідники, навряд чи можливо, з огляду на швидкий розвиток, зміну й удосконалення комп'ютерних технологій. КПК України наразі не виокремлює докази в електронній формі. Розглядаючи їх у контексті документів, законодавець поширив на докази в електронній формі загальні правила застосування доказів у кримінальному провадженні. Одночасно діє значна кількість міжнародних, регіональних і національних правових актів, ефективних практик, пов'язаних із правовим регулюванням використання доказів в електронній формі.

Зокрема, Міжнародна організація з комп'ютерних доказів (International Organization on Computer Evidence – IOCE) сформулювала низку принципів, яких має бути дотримано під час розслідувань злочинів, учинених із застосуванням комп'ютерів: після вилучення цифрових доказів учинені дії не мають змінювати такі докази; якщо особі потрібно одержати доступ до оригіналу цифрового доказу, ця особа має бути компетентною в цьому аспекті;

усі дії, пов’язані з вилученням, доступом, зберіганням або передачею цифрових доказів, мають бути повністю задокументовані, збережені й доступні для перегляду; особа несе відповідальність за всі дії, здійснені відносно цифрових доказів, поки такі докази знаходяться в її розпорядженні; будь-який орган, відповідальний за вилучення, доступ, зберігання або передачу цифрових доказів, несе відповідальність за дотримання цих принципів [111, с. 98–101].

Зосередимо увагу на постанові Верховного Суду від 13 липня 2020 року у справі № 753/10840/19, у якій суди дійшли двох висновків, а саме: висловлення погроз з боку колишнього чоловіка за допомогою Viber є психологічним насильством, а скриншоти з мобільних пристроїв можуть бути належним доказом учинення такого насильства. Під час розгляду справи представник відповідача акцентував, що надані заявником роздруківки містять лише імена людей, зокрема кривдника як відправника, проте не надано доказів, з якого саме мобільного номера та на які номери надсилали ці повідомлення, що унеможливлює встановлення відправника й 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 скриншоти електронного листування в застосунку Viber належними доказами психологічного насильства з боку відповідача [80].

А. Матвійчук стверджує, що електронні докази – інформація, яку було створено, збережено або передано в електронній формі, її може бути використано як доказ у кримінальному провадженні. До електронних доказів належать електронні листи, текстові повідомлення, аудіо- та відеозаписи, інформація із соціальних мереж, дані з мобільних пристроїв, комп’ютерів, серверів, а також інформація із хмарних сховищ [59, с. 239].

Електронні докази в цивільному процесі становлять єдність фактичних даних, що мають значення для правильного вирішення справи, та їх процесуальної форми, тобто засобів доказування.

Стосовно визначення правового режиму електронних доказів зауважимо, що загалом їх регулює спеціальний закон, у якому зазначено, що електронним документом є документ, інформація в якому зафіксована у вигляді електронних даних, зокрема обов'язкових реквізитів документа. Проаналізувавши чинне законодавство України та реальну практику використанням цих норм, можна дійти висновку, що електронні докази можуть бути подані в оригіналі, в електронній чи паперовій копіях. Законодавці не передбачили додаткових вимог до такого документа, зокрема, з огляду на відсутність таких вимог до звичайних письмових документів на паперовому носії. Наприклад, очевидно, що під час подання письмових доказів суд не вимагає від сторони довести, що його підписала саме та особа, яка в ньому зазначена, що зміст документа є цілісним, його не змінено чи спотворено. Натомість до електронних доказів цю вимогу застосовують.

Основною умовою допустимості електронного доказу до розгляду в цивільному судочинстві є наявність електронного підпису, що надає можливість максимально точно ідентифікувати особу, якій належить відповідний електронний документ. Проте, крім електронного підпису, обов'язковою є наявність реквізитів, що стосуються відповідного поданого електронного документа [81]. За наявності окреслених сукупних факторів електронний доказ вважають допустимим, він не викликає сумнівів стосовно його достовірності.

Вимога щодо закріплення електронного документа цифровим підписом визначена в Законі України «Про електронну комерцію» від 3 вересня 2015 року, у якому зазначено, що відповідний електронний правочин вважають підписаним з моменту використання електронного цифрового підпису [82]. Отже, такий аргумент доводить, що будь-який електронний документ має бути відповідно підписаний та завірений, щоб мати всі підстави для визнання його належно завіреним.

Вищий спеціалізований суд України з розгляду цивільних та кримінальних справ в ухвалі від 22 лютого 2017 року надав роз'яснення

стосовно допустимості доказів, розміщених у мережі Інтернет. Попередньо апеляційний суд не визнав допустимими електронні докази, одержані за допомогою проведення експертного дослідження телекомунікаційної системи щодо роздруківок текстів інформації з вебсайту телеканалу «112» і відповідних скриншотів відповідача. Таке рішення апеляційного суду скасовано, що свідчить про допустимість доказів, узятих і досліджених із мережі Інтернет [109].

Розглядаючи питання про застосування електронних доказів, прогалини як спосіб доказування та проблеми застосування їх на практиці, безумовно, слід зауважити, що:

– запровадження в ЦПК України такого нового самостійного засобу доказування, як електронний доказ, є позитивним явищем, адже воно надає можливість уникнути певних проблемних питань, що раніше виникали в судовій практиці, з огляду на нормативну неврегульованість застосування таких джерел доказової інформації;

– визначення терміна «електронні докази» є доволі широким і вдалим, тому що має невичерпний перелік видів електронних доказів та джерел їх зберігання.

Вивчаючи питання про недосконаліть правового регулювання, застосування електронних доказів учасниками судової справи, доходимо висновку, що:

1) подання електронних доказів, правила засвідчення як електронної копії електронного доказу, так і його паперової копії закон не передбачає;

2) несформованість єдиного підходу до видів електронних доказів у теорії процесуальних юридичних наук, наявні лише окремі класифікації;

3) нерозмежування копії та оригіналу електронних доказів.

Отже, у межах дослідження виокремлено головні прогалини, пов’язані з поданням, дослідженням й оцінюванням електронних доказів у цивільному судочинстві, унаслідок цього можна запропонувати певні шляхи їх усунення:

– для ефективного правового регулювання наділити нотаріуса правом належно засвідчувати електронні документи;

– чітко класифікувати електронні докази за їх внутрішнім змістовим наповненням;

– для уникнення фальсифікації електронних доказів розробити способи захисту;

– з огляду на недосконале визначення понять «оригінал електронного доказу» та «копія електронного доказу», внести зміни до ЦПК України, якими чітко розмежувати їх.

Ступінь захищеності доказів доволі низький, що зумовлює ігнорування судами значного обсягу доказів, які долучають сторони, з причини нібито недоведеності їх належності, допустимості й достовірності. У ЦПК України не передбачено механізму захисту електронних доказів від їх підроблення, зміни та виправлення інформації.

Слід зауважити про використання електронних доказів у законодавстві іноземних держав. Жодна європейська країна не має в кодифікованих актах прямого визначення електронних доказів. У Фінляндії засобами доказування є певні дії (як електронні, так і традиційні), дефініції не закріплено. У Цивільному кодексі Франції електронні документи є рівнозначними з письмовими. У ЦПК Греції доказами є будь-які реальні факти, що мають суттєве значення для вирішення спору. У Казахстані електронні докази вважають підвидом письмових доказів [4, с. 67–68].

Воєнний стан в Україні надає можливість, а інколи і змушує учасників судового процесу на вільних від збройних конфліктів територіях по-новому оцінити можливості, що надає підсистема «Електронний суд», що є складовою Єдиної судової інформаційно-телекомунікаційної системи. Законодавче закріплення електронних доказів як засобів доказування є своєчасним прогресивним кроком, передусім у тих умовах, у яких Україна знаходиться протягом тривалого проміжку часу [69, с. 278].

Тотальна цифровізація передбачає активне застосування ІТ-технологій, без яких уже не можуть розвиватися різноманітні напрями діяльності людства. Будь-яка сфера діяльності людини видозмінюється залежно від можливостей пристосовувати використання технічного прогресу під час виконання певних функцій. Не є винятком суспільні відносини, які виникають у сфері права. Можливості застосування результатів технічного прогресу наявні в повсякденному житті більшості людей, вони можуть виконувати ширший спектр дій, які ще в недалекому минулому були для них недосяжними. Наприклад, використання функціональних можливостей телефонів, зокрема відеокамери, дає змогу очевидцям події злочину записати відео обставин, які згодом стануть доказами в кримінальному провадженні. Слід констатувати, що, на жаль, механізми внесення змін до законодавства України, яке врегульовує кримінально-процесуальні відносини, є повільними та не відповідають вимогам сучасного суспільства. Внесені зміни й доповнення до КПК України можна назвати лише такими, що пов’язані з електронними доказами та не є комплексними, а тому не вирішують низку питань застосування електронних доказів як доказів вчинення правопорушення. Тому суд, оцінюючи електронні докази, заповнює відповідні прогалини за рахунок уже сформованої попередньої судової практики, що ґрунтується на правових нормах (які хоч і фрагментарно, однак закріплюють застосування електронних доказів у кримінальному процесі), а також аналогії права (за потреби). Зауважимо, що електронні докази дедалі частіше стають предметом судової оцінки. У частині випадків електронні докази можуть вказувати на основний факт вчинення кримінального правопорушення і бути головними в контексті достатності під час прийняття рішення по суті кримінального провадження. Також під час розслідування злочинів (наприклад, у кіберпросторі) можуть траплятися ситуації, де доказову базу формують тільки електронні докази.

У ЦПК України електронним доказам присвячено параграф 5 глави 5 «Докази та доказування». У ст. 100 цього Кодексу чітко визначено, як саме слід визначати поняття електронних доказів. У ч. 2 ст. 100 ЦПК України

закріплено можливість подавати електронні докази як в оригіналі, так і копії, зокрема може бути подано паперову копію електронного доказу, що має бути відповідно посвідчена згідно з вимогами чинного законодавства (копія електронного доказу може бути не взята судом до уваги в разі сумніву щодо її відповідності оригіналу) [115]. Також поняття електронних доказів і деякі питання, пов'язані з порядком їх зберігання, подачі в суд оригіналу чи копії електронних доказів, закріплено в ст. 96 параграфа 5 глави 5 «Докази та доказування» Господарського процесуального кодексу України [25]. На жаль, у КПК окремої статті про електронні докази немає.

Оскільки в кримінальному процесуальному законодавстві недостатньо закріплено питання стосовно застосування електронних доказів, судова практика частково допомагає зрозуміти, як саме слід застосовувати такі докази, що фактично існують з тенденцією до збільшення. З огляду на зазначене, доцільно акцентувати на правовій оцінці електронних доказів учинення злочину, зокрема судовій оцінці.

У кримінальному процесі оцінку доказів здійснюють слідчий, прокурор, слідчий суддя, суд за внутрішнім переконанням відповідно до вимог ст. 94 КПК України [53].

Видається доцільним розглянути окремі рішення судів саме касаційної інстанції, тому що така оцінка доказів є кінцевою під час вирішення спірних питань щодо визнання доказу допустимим у кримінальному провадженні.

Згідно зі ст. 90 КПК України, суд може застосовувати рішення національного суду або міжнародної судової установи в питаннях допустимості доказів, що має для нього преюдиціальне значення: суд може прийняти беззаперечними обставини (юридичні факти), що були встановлені іншим судом в іншій справі [53].

Судді виконують головну роль під час оцінки електронних доказів. Саме від їх компетенції та рішення залежить, чи буде доказ, зокрема електронний, відігравати ключову роль у вирішенні конкретної справи.

З огляду на важливість судової практики в питаннях оцінки електронного доказу на предмет його допустимості, необхідно зосередити увагу на деяких тезах судових рішень:

– запис телефонної розмови є допустимим доказом за умови, що на телефоні працює програма автоматичного запису всіх розмов його власника;

– розмова, зафіксована потерпілим на диктофон, є недопустимим доказом, якщо запис було здійснено цілеспрямовано;

– відеозаписи, здійснені за допомогою системи відеоспостереження міста, є допустимими доказами та не мають ознак проведення НСРД, тому що фіксація за допомогою цієї системи є відкритою та спрямована на спостереження за визначеними об’єктами;

– належно оформленими джерелами фактичних даних (доказів) є перенесені записи на компакт-дисках DVD-R, а саме копії тих оригінальних даних (записів НСРД), які фіксували технічними засобами під час проведення аудіо-, відеоконтролю;

– долучений слідчим до матеріалів провадження як речовий доказ DVD-R диск з відеозаписом обставин події є самостійним джерелом доказу, похідним від інформації, що зберігається на комп’ютері в електронному вигляді у формі файлів. Тому записаний на оптичний диск (носій інформації) електронний файл у вигляді відеозапису є оригіналом (відображенням) електронного документа;

– диски, які були виготовлені спеціалістами і не є первинними носіями інформації, проте містять аудіо-, відеофайли НСРД, є оригіналами електронного документу й допустимими доказами;

– протокол аудіо-, відеоконтролю особи передбачає обов’язкову наявність додатків з аудіо-, відеозаписами, однак якщо їх прокурор не надав суду (оптичні носії та карту пам’яті), це спричинить визнання цього доказу недопустимим;

– факт належного повідомлення сторони захисту про закінчення досудового розслідування та надання доступу до матеріалів досудового розслідування не підтверджують дані представлених прокурором фотоілюстрацій повідомлень з мобільних месенджерів WhatsApp і Telegram з телефона слідчого, оскільки за нікнеймом і соціальним профілем неможливо ідентифікувати особу, якій їх було надіслано. Крім цього, зі змісту фотоілюстрації щодо обміну повідомленнями неможливо достеменно встановити дату надіслання та одержання таких повідомлень.

Такі варіанти оцінки електронних доказів суди аргументували положеннями закону та сформованою судовою практикою, яка проглядається в частині викладу мотивів суду прийняття рішення, серед яких необхідно зазначити такі:

– «ототожнення електронного доказу як засобу доказування та матеріального носія такого документа є безпідставним, тому характерною рисою електронного документа є відсутність жорсткої прив’язки до конкретного матеріального носія»;

– «у випадку зберігання інформації на кількох електронних носіях кожний з електронних примірників вважають оригіналом електронного документа»;

– «основною особливістю електронного документа є відсутність жорсткої прив’язки до конкретного матеріального носія, який є тільки способом збереження інформації та має значення лише тоді, коли електронний документ є речовим доказом»;

– «один і той самий електронний документ (відеозапис) може існувати на різних носіях, а всі ідентичні за змістом примірники електронного документа можна розглядати як оригінали, вони різняться лише часом і датою створення»;

– «питання ідентифікації електронного документа як оригіналу можуть бути вирішені вповноваженою особою, яка його створила (за допомогою спеціальних програм обчислюють контрольну суму файлу чи

каталогу з файлами: CRC-сума, hash-сума), або за наявності відповідних підстав шляхом проведення спеціальних досліджень» [3, с. 27–29].

Розглянемо доктрину електронних доказів у кримінальному процесі, зокрема національні особливості та світові тенденції. Н. Зільник стверджує, що останніми роками відбувається постійне розширення інформаційних систем у світі. Цифрові технології активно застосовують у повсякденному житті, що призводить до модернізації різних сфер суспільного життя та виробництва. Прогрес у сфері інформаційних технологій є однією з головних складових глибоких трансформацій у державному секторі, метою яких є створення єдиного інформаційного простору з об'єднаною базою даних і розвинутою системою комунікацій. Інформаційно-телекомунікаційні технології дедалі активніше використовують у цивільному судочинстві для подання інформації в нових форматах та її використання як доказів. Ці технології допомагають точніше визначити місце інформації в системі доказів [34, с. 197].

Традиційно переважна частина доказів мала фізичну форму, наприклад, паперові документи, знаряддя вчинення кримінального правопорушення тощо. Однак з появою засобів інформаційно-комп'ютерних технологій (смартфонів, планшетів, ноутбуків тощо), які злочинці почали використовувати з протиправною метою, виникає новий вид доказів – електронні. Наприклад, один із перших зафіксованих випадків, пов'язаних зі злочинним застосуванням комп'ютера, стався 1966 року в штаті Міннеаполіс (США). Програміст М. А. Беннет, маючи доступ до комп'ютерної системи Національного міського банку Міннеаполіса, написав код, який змінив програмне забезпечення так, що у звітах не відображалося перевищення кредитного ліміту на його особистому рахунку. Це давало йому змогу незаконно користуватися коштами банку з власною метою. У зв'язку з виходом з ладу комп'ютерної системи, банк вимушений був повернутися до ручної обробки звітів, що й дало змогу виявити невідповідності на рахунку Беннета. За результатами проведеного ФБР розслідування, у січні 1967 року

Беннет одержав умовний строк. Цю справу в історії вважають першою, що пов'язана зі злочинним застосуванням комп'ютера [65; 142].

Судові органи вперше постали перед новими для того часу злочинними виявами, що були пов'язані з необхідністю дослідження електронних даних як доказів. Особливої актуальності питання дослідження електронних доказів набуває і в наш час. Аналізуючи визначення поняття «електронний доказ», слід зазначити, що в науковій літературі також використовують такі поняття: «цифровий доказ», «електронно-цифровий доказ», «електронний (цифровий) доказ» тощо. Оминаючи наукові дискусії з приводу використання зазначених понять, вважаємо за доцільне використовувати термін «електронний доказ», тому що в міжнародних нормативних актах, зокрема в актах Європейського Союзу, переважно використовують термін electronic evidence (електронний доказ) [152]. Попри те, що в КПК України не міститься визначення поняття «електронних доказів», проте його наведено в КАС України, ГПК України та ЦПК України [65].

У ст. 99 КАС України електронними доказами є інформація в електронній (цифровій) формі, що має дані про обставини, що мають значення для справи, зокрема електронні документи (текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних й інші дані в електронній формі. Такі дані можуть зберігати, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (зокрема в мережі Інтернет) [53]. Схожі визначення поняття електронних доказів містяться і в ст. 96 ГПК України та ст. 100 ЦПК України.

Відсутність визначення поняття електронних доказів у КПК України можна пояснити тим, що законодавець не наважується вносити відповідні зміни в кримінальне процесуальне законодавство, а продовжує традиційно

застосовувати дефініції «документи» та «речові» докази, розглядаючи електронні докази як їх аналоги й не виокремлюючи їх.

Відповідно до ст. 99 КПК України, електронні докази вважають документами, а матеріальні носії, на яких вони розміщені, визнають речовими доказами. Документом є спеціально створений з метою збереження інформації матеріальний об'єкт, що має зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюють під час кримінального провадження. Крім того, до документів можуть належати: матеріали фотозйомки, звукозапису, відеозапису й інші носії інформації (зокрема комп'ютерні дані) [53].

Відсутність визначення терміна електронних доказів у кримінальному процесуальному законодавстві змушує судову практику самостійно напрацьовувати підходи до їх тлумачення та застосування.

Наприклад, у постанові колегії суддів Другої судової палати ККС ВС від 6 лютого 2024 року акцентовано, що ненадання стороною обвинувачення з будь-яких підстав протоколу проведення слідчого експерименту за участю потерпілого не може зашкодити справедливому судовому розгляду з огляду на те, що проведення цієї слідчої дії відбулося без порушення будь-яких прав і свобод людини, передбачених Конвенцією та Конституцією України, а наданий технічний носій інформації, на якому зафіксовано проведення цієї слідчої дії, за обставин цього кримінального провадження, є електронним доказом, на якому міститься інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи [77].

В іншій постанові колегії суддів Третьої судової палати ККС ВС від 12 червня 2024 року було зазначено, що головними доказами в кримінальних провадженнях стосовно злочинів проти основ національної безпеки України є електронні (цифрові) докази, до яких належать: матеріали фотозйомки, звукозапису, відеозапису й інші носії інформації (зокрема комп`ютерні дані), що містяться у відкритих (інтернет; різноманітні медіа; соціальні мережі) чи закритих мережах (приватні месенджери й телеграм-

канали; особисте листування із застосуванням комп'ютерної техніки й мобільних телефонів, флешносії, карти пам'яті тощо) [79].

2020 року було підготовлено проєкт Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів», де пропонували визначити в ст. 100-1 КПК України поняття «електронний доказ», який слід тлумачити як інформацію в електронній (цифровій) формі з відомостями, що можуть бути використані як доказ факту чи обставин, що встановлюють під час кримінального провадження.

Цей законопроєкт у січні 2021 року було прийнято в першому читанні за основу та направлено Комітету Верховної Ради України з питань правоохоронної діяльності на доопрацювання з огляду на зауваження та пропозиції.

У низці іноземних країн поняття «електронних доказів» закріплено в кримінальному процесуальному законодавстві. Зокрема, відповідно до ст. 136 КПК Латвії, електронними доказами в кримінальному провадженні можуть бути факти у вигляді обробленої електронної інформації, що зберігається або передається автоматизованими пристроями чи системами обробки даних. У КПК Угорщини (ст. 205) наводять визначення «електронних даних» – це будь-яке представлення фактів, інформації та термінів, що придатне для технічної обробки інформаційною системою, зокрема будь-якої програми, яка реалізує функцію інформаційної системи. У Сінгапурі діє закон «Про докази», що врегульовує правила прийнятності доказів у судових процесах, зокрема в кримінальному провадженні. Він містить положення стосовно електронних записів та їх використання як доказів у суді. Електронним записом слід вважати запис, створений, переданий, одержаний або збережений за допомогою електронних, магнітних, оптичних або інших засобів в інформаційній системі або переданий з однієї інформаційної системи в іншу. Також у цьому законі містяться критерії застосування електронних доказів (116A) у кримінальному провадженні: 1) якщо не надано доказів, що засіб,

який створив певний файл, зазнав змін, то записаний файл є належним і допустимим доказом; 2) якщо запис був створений третьою особою, яка не є стороною в кримінальному провадженні, то цей запис є належним і допустимим доказом; 3) якщо запис був створений стороною провадження, а інша сторона заперечує цей доказ, то доказ вважають належним і допустимим [65].

Т. Фоміна вважає, що XXI ст. – епоха розвитку інформаційних технологій. Технологічний прогрес пронизує всі сфери нашого життя. Складно уявити побут сучасної людини без використання електронних пристроїв, гаджетів, адже вони стали своєрідним атрибутом сьогодення. Наприклад, популярність мобільного телефону зумовлена його компактністю та функціональністю, яких досягають за рахунок можливості прийому дзвінків, виходу в мережу Інтернет, здійснення фото-, відеозйомки й навіть використання телефону як файлової системи. Оскільки електронні пристрої стали архівом публічних і приватних даних, правоохоронні органи почали застосовувати гаджети як можливість одержання інформації. Навіть за умови, коли електронний пристрій не використовував злочинець, дії правопорушника могли потрапити на камери відеоспостереження або перебування особи на місці події могло бути зафіксовано за допомогою глобальної системи позиціювання (GPS). Інформація, одержана з електронних пристроїв, може бути використана для побудови слідчих версій, встановлення злочинних зв’язків і навіть для підтвердження факту вчинення злочину [112, с. 207–208].

У Великій Британії також є окремий нормативний акт – «Про кримінальне правосуддя (Criminal Justice Act 2003), у якому не визначено поняття електронних доказів, однак встановлено презумпцію (правило) належної роботи пристрою. Відповідно до положень нормативного акта, механічні або автоматизовані пристрої працюють належно, якщо не доведено протилежне. Наприклад, у справі Публічного обвинувачення проти Вільяма Елліотта та Роберта Маккі (2013) (The Public Prosecution Service v. William Elliott and Robert McKee), яких було заарештовано за підозрою в крадіжці

будівельних матеріалів, під час розслідування поліція використала електронний пристрій для зняття відбитків пальців – Livescan. Відбиток великого пальця Елліотта збігся з відбитком, знайденим на місці вчинення кримінального правопорушення. Проте на момент використання пристрій Livescan не був офіційно затверджений Державним секретарем, відповідно до вимог Порядку поліції та кримінальних доказів. Тому Верховний Суд зауважив, що скани відбитків пальців, одержані за допомогою електронного зчитувача Livescan, були допустимими доказами, навіть якщо на той час цей пристрій не був схвалений Державним секретарем. Це рішення засвідчує, що в британській судовій практиці увагу зосереджують передусім на надійності й достовірності електронних доказів, а не тільки на формальних процедурах їх одержання. Отже, навіть за відсутності офіційного затвердження пристрою одержані за його допомогою докази можуть бути визнані допустимими, якщо їх достовірність не викликає сумнівів [65].

У Сполучених Штатах Америки діє закон «Федеральні правила доказування». У цьому нормативному акті поняття електронного доказу не визначено. Проте в п. 5 ст. 101 окреслено головні терміни, а також зазначено, що посилання на будь-який вид письмового матеріалу чи будь-яке інше середовище охоплює електронно збережену інформацію. У Законі (ст. 901) встановлено процес аутентифікації (підтвердження) доказів. Для того щоб задовольнити вимогу аутентифікації або ідентифікації предмета доказів, сторона, що подає доказ, має надати достатньо доказів для підтвердження того, що предмет є тим, чим його заявлено. Крім цього, у законі закріплено вимогу про достовірність електронних доказів. Зокрема, такими є записи, створені електронними процесами або системами, які дають точний результат і сертифіковані уповноваженою особою. Слід зауважити, що процес сертифікації передбачає надання відповідного документа, у якому підтверджено достовірність даних або записів. Це може бути сертифікат, підписаний особою, яка бере на себе відповідальність за правильність і достовірність цього запису. Наприклад, представник організації (IT-

менеджер), що зберігає електронні дані, може видати сертифікат про те, що файл або електронний запис було створено, збережено та зафіксовано в межах звичайної діяльності цієї організації. Сертифікат містить відомості про час створення файлу, його автентичність і відсутність змін з моменту створення. Якщо прокурор надає як доказ електронні дані, вилучені із жорсткого диска сервера чи комп'ютера підозрюваного/обвинуваченого, у цьому разі технічний експерт, що працював із жорстким диском, надає сертифікат, який підтверджує, що дані було скопійовано з оригінального пристрою за допомогою процесу цифрової ідентифікації. Експерт зазначає, що методи копіювання не змінили зміст даних [65].

З огляду на міжнародну практику країн Європейського Союзу щодо електронних доказів у кримінальному провадженні, суди використовують низку критеріїв, які гарантують їх достатність і допустимість, серед яких: 1) законність одержання. Докази мають бути зібрані відповідно до законодавства, без порушення прав людини; 2) автентичність і цілісність. Необхідно підтвердити, що доказ є оригінальним і не був змінений з моменту його отримання. Електронні докази мають бути збережені в первісному стані без жодних змін; 3) допустимість і релевантність (належність). Доказ має відповідати процесуальним вимогам для його прийняття в суді. Суд і сторони повинні мати доступ до обладнання та програмного забезпечення, необхідного для роботи з електронними доказами. Доказ має безпосередньо стосуватися справи та підтверджувати або спростовувати обставини, які розглядають; 4) ланцюг збереження. Має бути забезпечено документування кожного етапу роботи з електронними доказами: хто, коли і за яких умов їх вилучив, зберігав й аналізував; 5) технологічна нейтральність. Принципи застосовують до всіх типів електронних доказів, незалежно від платформи або технології, які використовували [65, с. 255–259].

З огляду на невпинний розвиток технологій, що породжує появу нових прийомів з'ясування фактів й обставин, що мають значення для кримінального

провадження та підлягають доказуванню, розширення системи процесуальних джерел доказів є неминучим.

Отже, електронні докази, за умови їх технічної надійності, можуть мати фактичні дані, що належать до обставин, які підлягають доказуванню в кримінальному провадженні. У таких випадках правова оцінка суду доказового значення такої інформації, законного порядку її збирання та застосування в матеріалах кримінального провадження є вагомою. Вивчення судової практики стосовно питань, пов'язаних з електронними доказами, на сучасному етапі розвитку інституту електронних доказів у кримінальному процесі є необхідним як для створення рекомендацій стосовно діяльності на етапі досудового розслідування, так і для використання законодавцем під час законотворчої роботи в питаннях внесення відповідних доповнень до КПК України.

На підставі аналізу міжнародного законодавства та практики можна запропонувати такі шляхи впровадження електронних доказів у кримінальне процесуальне законодавство України: 1) закріплення поняття електронних доказів у КПК України, унормування його визначення та переліку того, що саме можна вважати електронними доказами; 2) створення окремого закону, який буде визначати процедуру дослідження, збирання, зберігання та аналізу електронних доказів; 3) встановлення чітких і зрозумілих процедур належності й допустимості електронних доказів у кримінальному провадженні [65].

Висновки до розділу 3

1. Позитивно оцінено зміни, внесені до ч. 4 ст. 99 КПК України, згідно з якою копії інформації (зокрема комп'ютерних даних), отримані слідчим або прокурором із залученням спеціаліста, суд визнає як оригінал документа. Аналізована норма фактично легалізує застосування криміналістичних

методів копіювання цифрових даних й означає, що якщо слідчий за участю спеціаліста з інформаційних технологій скопіює потрібні файли з комп'ютера чи іншої електронної системи на окремий носій, ця копія матиме таку саму доказову силу, що й початковий носій інформації. Тобто законодавець відійшов від імперативної вимоги обов'язкового вилучення технічних засобів (серверів, мобільних пристроїв) і дозволив використання належно завірених копій електронних документів як джерела доказів. Таке законодавче бачення забезпечує необхідний баланс між ефективністю досудового розслідування та захистом майнових прав володільців техніки, обмежуючи вилучення оригіналів пристроїв лише випадками об'єктивної необхідності.

Водночас акцентовано на недоліках аналізованого вище законодавчого положення, що полягають у браку детальної процедури долучення, реєстрації та зберігання таких електронних доказів у матеріалах кримінального провадження з визначенням кола відповідальних осіб.

2. Запропоновано алгоритм вилучення цифрового носія, що передбачає: 1) вчинення дій, що унеможливлюють зміну даних на ньому після вилучення (наприклад, вимкнення живлення комп'ютера, використання спеціальних блокувальних пристроїв для портів, поміщення смартфона в екранований контейнер для блокування сигналів тощо); 2) фіксацію всіх обставин, пов'язаних із вилученням, а саме: час вилучення, коло осіб, які мали доступ, серійні номери техніки, стан пристрою (ввімкнений чи вимкнений), наявність запаролення або шифрування тощо; 3) невідкладне дублювання даних (створення копії) у присутності понятих або з використанням безперервного відеозапису із залученням ІТ-спеціаліста.

3. Акцентовано на технічній стороні збереження електронних даних. У зв'язку з цим увагу зосереджено на запровадженні в Україні позитивного досвіду США в частині розроблення детальних інструкцій для «першого реагування» на місці вилучення електроніки (First Responder Guides), які регламентують найдрібніші деталі – від порядку фотографування екрана

ввімкненого комп'ютера до порядку вилучення інформації із «хмари» через провайдера.

4. На підставі аналізу судових рішень зафіксовано поступову трансформацію судової практики в питаннях використання електронних доказів у кримінальному провадженні від їх сприйняття як різновиду документів до визнання самостійним джерелом доказової інформації. Основні зміни в підходах судів до електронних доказів стосуються: 1) упровадження сталих критеріїв оцінки цифрових даних (автентичність, цілісність, належність і допустимість); 2) розширення кола допустимих електронних доказів (від відеозаписів камер спостереження до скриншотів із месенджерів, GPS-координат чи метаданих файлів); 3) оцінки таких матеріалів з огляду на презумпцію їх надійності, якщо не доведено протилежне. Водночас брак дефініції «електронні докази» в положеннях Кримінального процесуального кодексу України призводить до неоднозначності правозастосування цього інституту.

5. У контексті опрацювання судової практики здійснено порівняльний аналіз використання електронних доказів у суміжних видах судочинства, що дав змогу виокремити основні прогалини, пов'язані з поданням, дослідженням й оцінкою електронних доказів у цивільному процесі та запропонувати шляхи їх усунення: 1) для ефективного правового регулювання наділити нотаріуса правом належно засвідчувати електронні документи; 2) чітко класифікувати електронні докази за їх внутрішнім змістовим наповненням; 3) для уникнення фальсифікації електронних доказів розробити способи захисту; 4) з огляду на недосконале визначення понять «оригінал електронного доказу» та «копія електронного доказу», внести зміни до ЦПК України, якими чітко розмежувати їх.

6. Вивчення рішень національних судів надає можливість визначити такі основні підходи в частині оцінки електронних доказів: 1) розмежування змісту та носія (суди обґрунтовано акцентують на безпідставності ототожнення електронного доказу з його фізичним носієм); 2) множинність оригіналів (у

разі зберігання інформації на кількох електронних носіях кожний з електронних примірників вважають оригіналом електронного документа); 3) відсутність жорсткої прив'язки електронного документа до конкретного матеріального носія, який є тільки способом збереження інформації та має значення лише тоді, коли електронний документ є речовим доказом; 4) питання ідентифікації електронного документа як оригіналу можуть бути вирішені вповноваженою особою, яка його створила (за допомогою спеціальних програм обчислюють контрольну суму файлу чи каталогу з файлами: CRC-сума, hash-сума), або за наявності відповідних підстав шляхом проведення спеціальних досліджень.

ВИСНОВКИ

У дисертаційному дослідженні розроблено основні теоретико-правові положення, пропозиції та практичні рекомендації щодо належності й допустимості електронних доказів у кримінальному провадженні, що мають значення для науки й практики кримінального процесу, зокрема:

1. З’ясовано, що в доктрині кримінального процесу електроні докази тлумачать як: носії інформації, що потребує спеціальних процедур фіксації, збереження та перевірки достовірності (О. Капліна, М. Шумило, Р. Юрка); фактичні дані, що зберігаються в електронному вигляді на будь-яких видах носіїв і стають доступними для сприйняття людиною після обробки спеціальними технічними засобами та програмним забезпеченням (Д. Алєксєєва-Процюк, О. Брисковська); інформацію (відомості), що мають електронну (цифрову) форму про обставини, які підлягають обов’язковому доказуванню в кримінальному провадженні (С. І. Хом’яченко, Т. О. Часова).

Констатовано, що на дисертаційному рівні висвітлення змісту електронних доказів зосереджено в роботах О. Ю. Гусєва («Електронні докази у цивільному процесі України», 2021), А. В. Скрипника («Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні», 2021), І. Г. Каланчі («Докази електронної форми у кримінальному процесі України: теорія та практика», 2025). Попри різні бачення науковців щодо поняття, значення, класифікації та інших аспектів електронних доказів, у працях останніх років простежується спільна думка про те, що докази в електронній формі мають особливу природу, яка відрізняє їх від традиційних матеріальних доказів, і це обґрунтовує їх самостійне місце в системі процесуальних джерел доказів.

2. Визначено, що оригіналом електронного технічного документа є той, який створений та зберігається на первинному носії інформації, натомість дублікатом (копією) є його копіювання, переміщення, поширення на інші носії даних. Акцентовано, що роздруківка вебсторінки, частини відео, фото чи

іншого файлу не можуть бути визнані ні оригіналом, ні копією електронного документа та не мають самостійного доказового значення. Візуалізована в паперовій формі сторінка може бути тільки додатком до проведеної слідчої (розшукової) дії. Зауважено, що належне виготовлення дубліката електронного документа забезпечує його допустимість під час перевірки доказів у суді.

Окреслено питання, що потребують урегулювання, щодо використання електронних доказів у кримінальному процесуальному праві України, серед яких: невідмежованість електронного доказу від інших джерел доказів; невизначеність джерел одержання електронних доказів у кримінальному провадженні; недостатність нормативно-правового регулювання щодо застосування копії електронних доказів, оригінали яких утрачено; обмеження можливостей дізнавача стосовно застосування електронних доказів; неорганізованість роботи інформаційно-телекомунікаційної системи досудового розслідування за участю Національної поліції України.

3. На підставі дослідження міжнародного досвіду (Австрія, Болгарія, Велика Британія, Італія, Китайська Народна Республіка, Федеративна Республіка Німеччина, Португалія, США, Чехія, Франція, Швеція) з'ясовано, що в більшості країн електронні дані визнають повноцінним видом доказів, рівнозначним традиційним письмовим чи речовим доказам, незалежно від наявності спеціального визначення в національному законодавстві. З'ясовано, що хоча законодавство переважної більшості досліджуваних країн не містить специфічного закону про електронні докази в кримінальному процесі, зарубіжна правозастосовна практика фокусує увагу на важливості дотримання принципу незмінності даних (жодного редагування оригіналу), документування всіх дій з електронним носієм і використання належних методів цифрової криміналістики, дотримання встановлених процесуальних вимог і технічних стандартів, щоб гарантувати автентичність та цілісність даних.

Увагу зосереджено на несформованості уніфікованого міжнародного підходу до поняття, класифікації чи процедур поводження з електронними доказами, що ускладнює їх транскордонний обіг. У зв'язку з цим позитивно оцінено міжнародні акти ЄС (Регламент (ЄС) 2023/1543 про Європейські ордери на пред'явлення та збереження електронних доказів у кримінальному провадженні та Директиву (ЄС) 2023/1544), що набувають чинності 2026 року та передбачають можливість для судових органів однієї країни безпосередньо звертатися з європейським ордером до інтернет-сервіс провайдера, який діє на території іншої країни, без необхідності проходження традиційного міждержавного запиту; визначають категорії даних, які можуть запитувати (дані абонента, дані трафіка і контент); встановлюють гарантії захисту прав у вигляді вимоги щодо повідомлення держави – виконавця ордера, яка може відмовити у виконанні за певних обставин (наприклад, якщо це загрожує національним інтересам або суперечить основним правам). Ці міжнародні документи спрощують й уніфікують доступ до електронних доказів у межах Європейського Союзу, долаючи залежність від повільних процедур взаємної правової допомоги.

З'ясовано, що відповідно до практики ЄСПЛ збирання та оцінка електронних доказів передбачає дотримання права на повагу до приватного й сімейного життя. Питання порушення такого права слід розглядати з позиції «розумного очікування конфіденційності». Висвітлено основні позиції ЄСПЛ у частині досліджуваного питання, відповідно до яких: 1) у сферу захисту права, передбаченого ст. 8 Конвенції, потрапляють не лише особисті відносини, а й різноманітні аспекти цифрових комунікацій (телефонні дзвінки, електронні листи, повідомлення, відомості про користування інтернетом на робочому місці тощо); 2) будь-яка форма цифрового нагляду повинна мати чітке законодавче підґрунтя та відповідати критеріям передбачуваності (моніторинг цифрових комунікацій без жодного нормативного акта чи внутрішньої політики не відповідає «вимозі передбаченості закону»); 3) втручання повинно бути необхідним у демократичному суспільстві, мати

законну мету («охорона національної безпеки, запобігання злочинам, захист прав жертв») і бути пропорційним обставинам («серйозність злочинів й обмежений характер спостереження»).

4. Встановлено, що електронні докази охоплюють широкий спектр інформації – від файлів і листувань у месенджерах до записів камер спостереження й даних із хмарних сховищ. Їх належність у кримінальному провадженні зумовлена зв'язком із предметом доказування, що потребує ретельної ідентифікації користувача, джерела походження та часових меж. Акцентовано на питанні автентичності, зокрема цифровий доказ слід вважати належним лише тоді, коли його можна об'єктивно пов'язати з подією, особою чи обставиною, які досліджують. Визначено «мінімальний стандарт» належності електронних доказів, що передбачає: ідентифікацію цифрових даних (зв'язок із користувачем/пристроєм/акаунтом), їх локалізацію (місце/сховище/сервіс), прив'язку в часі (timestamp/метадані) та відтворення (можливість отримати перевірну копію).

5. Констатовано, що допустимість електронних доказів залежить від суворого дотримання процесуальних вимог щодо їх отримання, фіксації та зберігання. З'ясовано, що судова практика під час вирішення питання про належність і допустимість електронних доказів встановлює: законність доступу/вилучення електронних документів, наявність підтвердження автентичності (електронний підпис, сертифікат, висновок експерта, хеш-суми) забезпечення рівності сторін (можливість огляду копії або оригіналу стороною захисту). У цьому контексті зазначено, що порушення порядку вилучення чи копіювання даних, відсутність судового дозволу на доступ або технічні помилки під час обробки носіїв неминуче призводять до ризику визнання доказу недопустимим. Водночас на практиці законодавець поступово формує підхід, орієнтований на мінімізацію вилучення обладнання та акцент на копіюванні інформації, що сприяє запобіганню зловживанням і забезпеченню балансу між інтересами слідства та правами власників техніки.

Аргументовано важливість дотримання принципу «ланцюга збереження доказів» (chain of custody), відповідно до якого кожен етап роботи з електронними даними (виявлення, копіювання, зберігання та передача) має бути задокументовано й перевірено. Зазначено, що використання технічних методів підтвердження автентичності (електронні підписи, контрольні хеш-суми, форензичні образи) створює підґрунтя для визнання доказів достовірними й виключає можливість їх непомітної модифікації. Брак зазначеного технічного підтвердження зумовлює ускладнення судової оцінки цифрових доказів.

6. У контексті дослідження питання допустимості й належності електронних доказів окреслено зміст стандартів доказування, які у фаховій літературі диференціюють залежно від стадії кримінального провадження: «обґрунтована підозра» (мінімальний рівень переконливості, необхідний для початку кримінального переслідування); «достатня підстава» (проміжний рівень, що зумовлює можливість прийняття процесуальних рішень); «поза розумним сумнівом» (найвищий стандарт, без досягнення якого постановлення обвинувального вироку є неможливим).

7. Позитивно оцінено зміни, внесені до ч. 4 ст. 99 КПК України, згідно з якою копії інформації (зокрема комп’ютерних даних), отримані слідчим або прокурором із залученням спеціаліста, суд визнає як оригінал документа. Аналізована норма фактично легалізує застосування криміналістичних методів копіювання цифрових даних та означає, що якщо слідчий за участю спеціаліста з інформаційних технологій скопіює потрібні файли з комп’ютера чи іншої електронної системи на окремий носій, ця копія матиме таку саму доказову силу, що й початковий носій інформації. Отже, законодавець відійшов від імперативної вимоги обов’язкового вилучення технічних засобів (серверів, мобільних пристроїв) і дозволив використання належно завірених копій електронних документів як джерела доказів. Таке законодавче бачення забезпечує необхідний баланс між ефективністю досудового розслідування та

захистом майнових прав володільців техніки, обмежуючи вилучення оригіналів пристроїв лише випадками об’єктивної необхідності.

Водночас увагу зосереджено на недоліках аналізованого вище законодавчого положення, що полягають у браку детальної процедури долучення, реєстрації та зберігання таких електронних доказів у матеріалах кримінального провадження з визначенням кола відповідальних осіб.

Запропоновано алгоритм вилучення цифрового носія, що передбачає: 1) вчинення дій, що унеможливлюють зміну даних на ньому після вилучення (наприклад, вимкнення живлення комп’ютера, використання спеціальних блокувальних пристроїв для портів, поміщення смартфона в екранований контейнер для блокування сигналів тощо); 2) фіксацію всіх обставин, пов’язаних із вилученням, а саме: час вилучення, коло осіб, які мали доступ, серійні номери техніки, стан пристрою (ввімкнений чи вимкнений), наявність запаролення або шифрування тощо; 3) невідкладне дублювання даних (створення копії) у присутності понятих або з використанням безперервного відеозапису із залученням ІТ-спеціаліста.

Акцентовано на технічній стороні збереження електронних даних. У зв’язку з цим увагу спрямовано на запровадження в Україні позитивного досвіду США в частині розроблення детальних інструкцій для «першого реагування» на місці вилучення електроніки (First Responder Guides), які регламентують найдрібніші деталі – від порядку фотографування екрана ввімкненого комп’ютера до порядку вилучення інформації із «хмари» через провайдера.

8. На підставі аналізу судових рішень зафіксовано поступову трансформацію судової практики в питаннях використання електронних доказів у кримінальному провадженні від їх сприйняття як різновиду документів до визнання самостійним джерелом доказової інформації. Основні зміни в підходах судів до електронних доказів стосуються: 1) упровадження сталих критеріїв оцінки цифрових даних (автентичність, цілісність, належність і допустимість); 2) розширення кола допустимих електронних

доказів (від відеозаписів камер спостереження до скриншотів із месенджерів, GPS-координат чи метаданих файлів); 3) оцінки таких матеріалів з огляду на презумпцію їх надійності, якщо не доведено протилежне. Водночас брак дефініції «електронні докази» в положеннях Кримінального процесуального кодексу України призводить до неоднозначності правозастосування цього інституту.

У контексті опрацювання судової практики проведено порівняльний аналіз використання електронних доказів у суміжних видах судочинства, що дав змогу виокремити основні прогалини, пов'язані з поданням, дослідженням й оцінюванням електронних доказів у цивільному процесі та запропонувати шляхи їх усунення: 1) для ефективного правового регулювання наділити нотаріуса правом належно засвідчувати електронні документи; 2) чітко класифікувати електронні докази за їх внутрішнім змістовим наповненням; 3) для уникнення фальсифікації електронних доказів розробити способи захисту; 4) з огляду на недосконале визначення понять «оригінал електронного доказу» та «копія електронного доказу», внести зміни до ЦПК України, якими чітко розмежувати їх.

Вивчення рішень національних судів дало змогу визначити такі основні підходи в частині оцінки електронних доказів: 1) розмежування змісту та носія (суди обґрунтовано акцентують на безпідставності ототожнення електронного доказу з його фізичним носієм); 2) множинність оригіналів (у разі зберігання інформації на кількох електронних носіях кожний з електронних примірників вважають оригіналом електронного документа); 3) відсутність жорсткої прив'язки електронного документа до конкретного матеріального носія, який є тільки способом збереження інформації та має значення лише тоді, коли електронний документ є речовим доказом; 4) питання ідентифікації електронного документа як оригіналу можуть бути вирішені уповноваженою особою, яка його створила (за допомогою спеціальних програм обчислюють контрольну суму файлу чи каталогу з файлами: CRC-сума, hash-сума), або за наявності відповідних підстав шляхом проведення спеціальних досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

5. Алєксєєва-Процюк Д. О., Бриськовська О. М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права.* 2018. Вип. 2. С. 247–253.

6. Ангеленюк А.-М. Ю. Використання електронних доказів у кримінальному процесуальному праві України (проблемні питання). *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2023. Вип. 79. Ч. 2. С. 214–218. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/10/34-1.pdf

7. Ангеленюк А.-М. Ю. Правова оцінка електронних доказів у кримінальному процесі України через призму судових рішень. *Південноукраїнський правовий часопис.* 2024. № 1. С. 26–30.

8. Андрієвська Л. О., Міцкевич В. О., Пащенко Ю. О. Електронні докази: вдале нововведення чи дефект законодавства. *Часопис цивілістики.* 2019. Вип. 35. С. 65–69.

9. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету.* 2016. № 36 (2). С. 123–125.

10. Ахтирська Н. М. Правова регламентація електронних доказів та практика їх використання в судочинстві України. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2023. Вип. 75 (2). С. 141–150.

11. Ахтирська Н. М. Процесуальні та організаційні аспекти збору електронних доказів за кордоном у межах міжнародного співробітництва. *Науковий вісник Ужгородського національного університету. Серія «Право».*

2022 Вип. 72. Ч. 2. С. 193–198. URL: https://dspace.uzhnu.edu.ua/server/api/core/bitstreams/4f8a8d7d-41fb-4aa5-9a01-6ec880404f65/content

12. Вапнярчук В. В. Допустимість доказів (доказування) в практиці Європейського Суду. *Публічне право*. 2015. № 2. С. 177–183.

13. Вапнярчук В. В. Теоретичні основи кримінального процесуального доказування : дис. … д-ра юрид. наук : 12.00.09. Харків, 2018. 524 с. URL: https://dspace.nlu.edu.ua/bitstream/123456789/15838/1/Vapnyarchuk_2018_dus.pdf

14. Вапнярчук В. В. Теорія і практика кримінального процесуального доказування : монографія. Харків : Юрайт, 2017. 408 с.

15. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Вид. 2-ге, доповн. Київ : Нац. акад. внутр. справ, 2020. 104 с. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/8e9e5637-7b62-475c-8c41-9850e317bfc4/content

16. Вирок Зарічного районного суду м. Суми від 28 квіт. 2016 р. Справа № 591/2665/15-к. Провадження № 1-кп/591/40/16. URL: http://reyestr.court.gov.ua/Review/57452822

17. Власова Г. П., Сафроняк Р. В. Допустимість і належність доказів за Кримінальним процесуальним кодексом України. *Вісник Національної академії прокуратури України.* 2014. № 1 (34). С. 26–32.

18. Гальченко В. С. Вилучення та процесуальне оформлення електронних доказів під час проведення досудового розслідування. *Вісник Кримінологічної асоціації України.* 2026. Т. 36. № 2 (Part I). С. 223–233. DOI: https://doi.org/10.32631/vca.2026.2.p1.17

19. Гальченко В. С. Докази й доказування в кримінальному процесі під час дії воєнного стану. *Кримінальне судочинство: права людини під час дії надзвичайного або воєнного стану* : матеріали Міжнар. наук.-практ. конф. (Київ, 18 листоп. 2022 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2022. С. 218–220.

20. Гальченко В. С. Електронні докази в кримінальному процесі. *Кримінальне судочинство: сучасний стан та перспективи розвитку* : матеріали Всеукр. наук.-практ. конф., присвяч. пам'яті проф. Ю. І. Азарова (Київ, 2 трав. 2024 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2024. С. 193–195.

21. Гальченко В. С. Міжнародно-правовий досвід використання електронних доказів як засобу доказування у кримінальному провадженні. *Науковий вісник Дніпровського державного університету внутрішніх справ*. 2026. № 1. С. 269–274. DOI: https://doi.org/10.32782/2078-3566-2026-1-35

22. Гальченко В. С. Особливості доказування на підставі електронних доказів: судова практика. *Вісник Кримінологічної асоціації України.* 2026. Т. 38. № 1 (Part II). С. 386–396. DOI: https://doi.org/10.32631/vca.2026.1.p2.35

23. Гальченко В. С. Проблемні питання допустимості електронних доказів на досудовому слідстві. *Кримінальне судочинство: сучасний стан та перспективи розвитку* : матеріали міжвідом. наук.-практ. конф. (Київ, 28 квіт. 2023 р.) / редкол.: С. С. Чернявський, Я. Ю. Конюшенко, В. В. Корольчук, Ю. В. Сухомлин. Київ : Нац. акад. внутр. справ, 2023. С. 43–46.

24. Гальченко В. С., Мурзо Є. О. Належність і допустимість електронних доказів, отриманих під час розслідування кримінального правопорушення за ст. 432 КК України. *Кримінальне процесуальне право на сучасному етапі розвитку України* : матеріали круглого столу, присвяч. 40-річчю кафедри крим. процесу (Київ, 27 жовт. 2023 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2023. С. 204–207.

25. Гарасимів О. І., Марко С. І., Ряшко О. В. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2023. Вип. 75. Ч. 2. С. 158–162. DOI: https://doi.org/10.24144/2307-3322.2022.75.2.25.

26. Главюк І. В., Степаненко А. С. Стандарт доказування «обґрунтована підозра» у кримінальному провадженні. *Правова позиція.* 2018. № 1. С. 13–20.

27. Главюк І., Завтур В. 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» № 2137-IX: аналіз новел кримінального провадження. *Вища школа адвокатури НААУ.* 2022. URL: https://www.hsa.org.ua/blog/zakon-ukrayiny-pro-vnesennya-zmin-do-kryminalnogo-protsesualnogo-kodeksu-ukrayiny-ta-zakonu-ukrayiny-pro-elektronni-komunikatsiyi-shhodo-pidvyshhennya-efektyvnosti-dosudovogo-rozsliduvannya-za-garyach

28. Головчук В. А. Проблемні питання належності доказів у кримінальному провадженні. *Аналітично-порівняльне правознавство.* 2026. Вип. 2. С. 73–77.

29. Господарський процесуальний кодекс України : Закон України від 6 листоп. 1991 р. № 1798-XII. URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text

30. Гусєв О. Класифікація електронних доказів у цивільному процесі України. *Підприємництво, господарство і право.* 2018. № 8. С. 18–22.

31. Гутник А., Хитра А. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : монографія. Львів : ЛьвДУВС, 2022. 204 с.

32. Гуцалюк М. В., Антонюк П. Є. Щодо сутності електронної (цифрової) інформації як джерела доказів в кримінальному провадженні. *Криміналістичний вісник.* 2020. № 1 (32). С. 37–49.

33. Дегтярьова О. Доказування у кримінальному провадженні на підставі електронних доказів. *Юридичний вісник.* 2021. № 6. С. 273–278.

34. Дєєв М. В. Визначення достатності доказів як складова частина процесу оцінки доказів. *Держава та регіони. Серія «Право»*. 2015. № 4. С. 65–74.

35. Дєєв М. В. Достатність доказів як передумова законності та обґрунтованості рішень у кримінальній справі. *Вісник Запорізького державного університету.* 2003. № 1. С. 1–2. URL: https://web.znu.edu.ua/herald/issues/archive/articles/2734.pdf?utm_source=chatgpt.com

36. Докази в кримінальному провадженні. URL: https://sa.dn.ua/files/dokazy_10072021.pdf

37. Завтур В. А. Особливості доказування при розгляді та вирішенні слідчим суддею та судом клопотань про застосування заходів забезпечення кримінального провадження : дис. … канд. юрид. наук : 12.00.09. Одеса, 2017. 237 с.

38. Зільник Н., Химинець М. Електронні докази в цивільному судочинстві: правова характеристика та особливості. *Вісник Національного університету «Львівська політехніка». Серія «Юридичні науки».* 2023. Т. 10. № 4. С. 196–205.

39. Ісланкін С. Актуальні питання доказування у кримінальному процесі. *Науковий вісник Дніпровського державного університету внутрішніх справ.* 2024. № 4. С. 187–191. DOI: https://doi.org/10.31733/2078-3566-2023-4-187-191

40. Каланча І. Г. Докази електронної форми у кримінальному процесі України: теорія та практика : дис. ... д-ра юрид. наук : 12.00.09. Київ, 2025. 617 с.

41. Каланча І. Г. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світлі концепції chain of custody. *Věda a perspektivy.* 2025. № 8 (51). С. 206–230.

42. Каланча І. Г. Окремі аспекти діяльності прокурора щодо гарантування цілісності доказів, що мають електронну форму під час досудового розслідування кримінального провадження. *Сучасні виклики та*

актуальні проблеми судової реформи в Україні : матеріали VI Міжнар. наук.-практ. конф. (Чернівці, 21 жовт. 2022 р.). Чернівці, 2022. С. 327–332.

43. Каланча І. Г. Організаційні аспекти роботи з доказами, що мають електронну форму в кримінальному процесі України. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2025. Вип. 90. Ч. 4. С. 258–266.

44. Каланча І. Г., Гаркуша А. М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал.* 2021. № 8. С. 336–339.

45. Каланча І. Г., Стемковський Д. Б. Використання доказів, що мають електронну форму, в кримінальному процесі України: судова практика. *Аналітично-порівняльне правознавство.* 2025. № 2. С. 1001–1008.

46. Капліна О. В. Проблеми допустимості доказів у кримінальному процесі. *Актуальні проблеми юридичної науки* : зб. тез Міжнар. наук. конф. «Десяті осінні юридичні читання» (Хмельницький, 18–19 листоп. 2011 р.). Хмельницький, 2011. Ч. 4 С. 51–53.

47. Квашук О. Д. Використання електронних доказів у кримінальному провадженні України: правова природа, процесуальні особливості та практика (із оглядом міжнародного досвіду). *Центральноукраїнський вісник права та публічного управління.* 2025. № 2. С. 50–56. DOI: https://doi.org/10.32782/cuj-2025-2-5

48. Коваленко А. В. Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренкаю.* 2018. № 4 (84). С. 237–245. DOI: 10.33766/2524-0323.84.237-245

49. Ковальчук С. О. Оцінка доказів судом у разі закриття кримінального провадження. *Доктринальні та правозастосовні проблеми кримінального процесу, детективної та оперативно-розшукової діяльності :* матеріали Міжнар. наук.-практ. конф., присвяч. 10-й річниці набуття чинності КПК України (Одеса, 9 груд. 2022 р.). Одеса : Одес. юрид. акад., 2022. С. 183–188.

50. Кодекс адміністративного судочинства України : Закон України від 6 лип. 2005 р. № 2747-IV. URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text

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

52. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини) : міжнар. док. від 4 листоп. 1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

53. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

54. Крет Г. Р. Міжнародні стандарти доказування у кримінальному процесі України: теоретико-правові та практичні основи : монографія. Калуш : Петраш К. Т., 2020. 452 с.

55. Крет Г. Р. Підстави визнання доказів недопустимими у контексті стандартів їх допустимості: законодавчий підхід і практика Верховного Суду. *Право.ua.* 2020. № 1. С. 131–137. DOI: https://doi.org/10.32782/law.2020.1.20

56. Крикунов О. В., Денісова Г. В. Загальні умови допустимості доказів у кримінальному провадженні. *Науковий вісник Ужгородського національного університету.* 2025. Вип. 87. С. 84–91.

57. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

58. Крицька І. О. Речові докази у кримінальному провадженні : дис. … канд. юрид. наук : 12.00.09. Харків, 2017. 249 с.

59. Лук’янчиков Є. Д., Лук’янчиков Б. Є. Допустимість як властивість доказів у кримінальному провадженні. *Науковий вісник Ужгородського національного університету.* 2025. Вип. 91. С. 355–361.

60. Малярова В. О. Належність та допустимість доказів у кримінальному провадженні. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2016. Вип. 38. Т. 2. С. 119–121.

61. Марочкін О. І. Поняття електронних доказів у кримінальному провадженні, їх види та класифікація. *Інтернаука. Серія «Юридичні науки».* 2024. № 10. С. 106–115.

62. Марчук Н. Про оцінку електронних доказів у кримінальному провадженні. *ADVOKAT POST*. 2024. URL: https://advokatpost.com/pro-otsinku-elektronnykh-dokaziv-u-kryminalnomu-provadzhenni-suddia-vs-kks-nataliia-marchuk/

63. Матвійчук А. В. Електронні докази у корупційних правопорушеннях. *Dictum Factum.* 2024. № 2 (16). С. 239–245. URL: https://df.duit.in.ua/index.php/dictum/article/view/360/323

64. Мельничук Ю. Л. Поняття допустимості доказів у кримінальному процесі. *Науковий вісник Ужгородського національного університету.* 2024. Вип. 86. С. 107–115.

65. Метелев О. П. Проблеми визначення допустимості і належності цифрових (електронних) доказів у кримінальному процесі. *Вісник кримінального судочинства.* 2019. № 3. С. 224–238.

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

67. Мілімко Л. В., Жидовцев Я. В. Електронні докази в кримінальному судочинстві України. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2025. Вип. 88. Ч. 3. С. 302–308. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/05/47-2.pdf

68. Мурадов В. В. Електронні докази: криміналістичний аспект використання. *Порівняльне правознавство.* 2013. № 3-2. С. 313–315.

69. Неділько Я. В. Доктрина електронних доказів у кримінальному процесі: національні особливості та світові тенденції. *Правова держава.* 2025. № 57. С. 254–262.

70. Ніколенко Л. М. Використання електронних доказів в кримінальному процесі зарубіжних країн. *Аналітично-порівняльне*

правознавство. 2024. № 5. С. 820–824. DOI: https://doi.org/10.24144/2788-6018.2024.05.125

71. Орлов Ю. Ю., Чернявський С. С. Використання електронних відображень як доказів у кримінальному провадженні. *Науковий вісник Національної академії внутрішніх справ.* 2017. № 3 С. 13–24. URL: http://elar.naiau.kiev.ua/jspui/handle/123456789/2392

72. Панова А. В. До питання поняття «допустимість доказів» у кримінальній процесуальній доктрині та законодавстві України. *Правове життя сучасної України :* матеріали Міжнар. наук. конф. Одеса : Фенікс, 2014. Т. 1. С. 716–718.

73. Парасюк М. В. Електронні докази у контексті принципів цивільного процесуального права. *Аналітично-порівняльне правознавство.* 2024. № 6. С. 277–281.

74. Петрик В. В. Використання електронних доказів у кримінальному провадженні: проблеми їх збору, перевірки та оцінки. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2025. Вип. 87 (4). С. 119–123.

75. Петрик В. В. Поняття та класифікація електронних доказів у кримінальному процесі у країнах світу. *Науковий вісник Ужгородського національного університету.* 2025. Вип. 90. С. 324–328.

76. Погорецький М. А. Допустимість доказів у кримінальному процесі та процесуальна доброчесність: доктрини і практика (порівняльно-правове дослідження). *Вісник кримінального судочинства.* 2025. № 1-1. С. 22–59.

77. Погорецький М. А. Нова концепція кримінального процесуального доказування. *Вісник кримінального судочинства.* 2015. № 3. С. 63–79.

78. Погорецький М. А. Сучасні концепції кримінального процесуального доказування. *Сучасні тенденції розвитку криміналістики та кримінального процесу.* Харків, 2017. С. 309–312. URL: https://univd.edu.ua/general/publishing/konf/08_11_2017/pdf/146.pdf

79. Погорецький М. А., Лисаченко Є. І. Допустимість доказів у кримінальному процесуальному праві країн Європейського Союзу та його вплив на допустимість доказів у кримінальному судочинстві України. *Вісник кримінального судочинства.* 2022. № 3–4. С. 20–34.

80. Погорецький М. А., Міцкан О. А. Стандарт доказування «достатня підстава» у кримінальному процесі України. *Вісник кримінального судочинства.* 2019. № 3. С. 31–42.

81. Постанова Верховного Суду колегії суддів Другої судової палати Касаційного кримінального суду від 6 лют. 2024 р. Справа № 645/6247/16-к. URL: https://reyestr.court.gov.ua/Review/116862907

82. Постанова Верховного Суду колегії суддів Першої судової палати Касаційного кримінального суду від 10 верес. 2020 р. Справа № 751/6069/19. Провадження № 51-1704км20. URL: https://reyestr.court.gov.ua/Review/91722819

83. Постанова Верховного Суду колегії суддів Третьої судової палати Касаційного кримінального суду від 12 черв. 2024 р. Справа № 569/190/23. Провадження № 51-1430 км 24. URL: https://iplex.com.ua/doc.php?regnum=119741340

84. Постанова Верховного Суду колегії суддів Третьої судової палати Касаційного цивільного суду від 13 лип. 2020 р. Справа № 753/10840/19. Провадження № 61-22727св19. URL: https://reyestr.court.gov.ua/Review/90385050

85. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

86. Про електронну комерцію : Закон України від 3 верес. 2015 р. № 675-VIII. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text

87. Ратнова А. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : дис. … д-ра філософії : 12.00.09. Львів, 2021. 248 с.

88. Ратнова А. В. Класифікація електронних документів, як джерел доказів у кримінальному провадженні. *Журнал східноєвропейського права.* 2021. № 84. С. 42–47. URL: http://nbuv.gov.ua/UJRN/jousepr_2021_84_9

89. Романюк В. В., Абламський С. Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі. *Право та безпека.* 2024. № 2. С. 140–150. DOI: https://doi.org/10.32631/pb.2024.2.13

90. Рябущенко Д. Ю. Концептуально-теоретична проблематика категорії «цифрових (електронних) доказів» у кримінальному процесі. *Економіка. Фінанси. Право.* 2023. № 5. С. 42–47.

91. Самойленко О. А., Чердинцев Ю. Г. Питання визнання джерелом доказів у кримінальному провадженні електронних (цифрових) документів. *Криміналістика і судова експертиза.* 2022. Вип. 67. С. 169–177.

92. Сенченко Н. М., Чумаченко В. Ю. Електронні докази у кримінальному провадженні: досвід реалізації у зарубіжних країнах. *Академічні візії.* 2025. Вип. 42. С. 1–10.

93. Сергєєва Д. Б. Допустимість доказів в теорії та КПК 2012 року. *Вісник кримінального судочинства.* 2015. № 3. С. 80–87.

94. Сергєєва Д. Б. Належність доказів за новим КПК України. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2013. № 3 (31). С. 234–239.

95. Сичевський В. В. Актуальні питання належності доказів у кримінальному провадженні. *Європейські перспективи.* 2015. № 4. С. 54–59.

96. Сичевський В. В. Правова природа гарантій належності і допустимості доказів у кримінальному судочинстві. *Наше право.* 2015. № 4. С. 73–78.

97. Сіренко О. В. Електронні докази у кримінальному провадженні. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2019. Вип. 14. С. 208–214.

98. Скрипник А. В. Використання інформації з електронних носіїв у кримінальному процесуальному доказуванні : дис. … д-ра філософії : 081 «Право». Харків, 2021. 369 с.

99. Слюсарчук Х. Р. Стандарти доказування у кримінальному провадженні : автореф. дис. … канд. юрид. наук : 12.00.09. Львів, 2017. 24 с.

100. Смирнов В. А. Допустимість як критерій оцінки доказів у кримінальному провадженні : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2021. 24 с.

101. Стахівський С. М. Теорія і практика кримінально-процесуального доказування : монографія. Київ, 2005. 272 с.

102. Степаненко А. С. Стандарт доказування «поза розумним сумнівом» у кримінальному провадженні : дис. … канд. юрид. наук : 12.00.09. Одеса, 2017. 234 с.

103. Степанов О. С. Належність та допустимість доказів в кримінальному процесі України : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2007. 16 с.

104. Столітній А. В., Каланча І. Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності.* 2019. Вип. 146. С. 179–191.

105. Стоянов М. М. Властивість належності доказів: поняття та зміст. *Актуальні проблеми держави і права*. 2011. Вип. 60. С. 204–209.

106. Стоянов М. М. Система правил допустимості доказів у кримінальному провадженні України. *Актуальні проблеми держави і права.* 2013. Вип. 70. С. 245–250.

107. Стратонов В. М. Використання цифрових технологій у виявленні та документуванні злочинів: досвід МКС та ЄСПЛ (аспекти електронних доказів). *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія «Юридичні науки»*. 2025. № 1. URL: https://juris.vernadskyjournals.in.ua/journals/2025/1_2025/30.pdf?utm_source=chatgpt.com

108. Тагієв С. Р. Проблемні питання правового регулювання використання електронних доказів у кримінальному процесі. *Академічні візії.* 2025. Вип. 41. С. 5–12. URL: https://academy-vision.org/index.php/av/article/view/1742/1623

109. Толочко О. Критерії визначення стандарту доказування вини поза розумним сумнівом у кримінальному провадженні. *Вісник Національної академії прокуратури України.* 2015. № 4 (42). С. 5−10.

110. Тютюнник В. В. Інститут допустимості доказів як гарантія ухвалення законного та обґрунтованого вироку суду : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2016. 20 с.

111. Уніфікація підходів до збору електронних доказів у кримінальному процесі України. *Судова влада України.* 2025. URL: https://court.gov.ua/archive/1746897/

112. Ухвала Апеляційного суду м. Києва від 29 черв. 2017 р. Справа № 760/15925/15-к. URL: https://zakononline.com.ua/court-decisions/show/67858013

113. Ухвала Вищого спеціалізованого суду України з розгляду цивільних та кримінальних справ від 22 лют. 2017 р. Справа № 761/13156/16-ц. URL: https://reyestr.court.gov.ua/Review/65038960

114. Ухвала Печерського районного суду м. Києва від 6 черв. 2018 р. Справа № 757/25582/18-к. URL: https://reyestr.court.gov.ua/Review/74568504

115. Фігурський В. М. Докази в електронній формі у кримінальному провадженні. *Галицькі студії. Серія «Юридичні науки».* 2023. Вип. 4. С. 97–105. DOI: https://doi.org/10.32782/galician_studies/law-2023-4-14

116. Фоміна Т. Г., Рачинський О. О. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Вісник Харківського національного університету внутрішніх справ.* 2023. № 3 (2). С. 207–220.

117. Хом’яченко С. І., Часова Т. О. Використання електронних доказів у кримінальному процесі. *Право. Людина. Довкілля.* 2020. Т. 11. № 2. С. 175–181.

118. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного*

університету. Серія «Юриспруденція». 2013. Вип. 5. С. 256–260. URL: http://nbuv.gov.ua/UJRN/ Nvmgu_jur_2013_5_58

119. Цивільний процесуальний кодекс України : Закон України від 18 берез. 2004 р. № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text

120. Чванкін С. А. Аудіо- та відеозаписи як різновид електронних доказів у цивільному процесі. *Теорія і практика правознавства.* 2020. Вип. 2. URL: http://nbuv.gov.ua/UJRN/tipp_2020_2_7

121. Чиж С. А. Правове регулювання доказування в кримінальному провадженні в умовах дії правового режиму воєнного стану. *Право.ua.* 2022. № 3. С. 258–264. DOI: https://doi.org/10.71404/law.ua.2022.3.37

122. Чиж С. А. Стандарт доказування «поза розумним сумнівом» у кримінальному провадженні. *Вісник Кримінологічної асоціації*. 2024. Т. 32. № 2. С. 983–993. DOI: https://doi.org/10.32631/vca.2024.2.77

123. Чупрікова І. Л. Допустимість доказів у світлі нового Кримінального процесуального кодексу : дис. ... канд. юрид. наук : 12.00.09. Одеса, 2016. 191 с.

124. Шило О. Г. Загальна характеристика показань як процесуального джерела доказів у кримінальному провадженні. *Вісник кримінального судочинства.* 2015. № 1. С. 151–156.

125. Шумило М. Є. Докази досудового і судового провадження в КПК України: співвідношення та їх функціональне призначення. *Право України.* 2013. № 11. С. 206–215.

126. Шумило М. Є., Юрка Р., Капліна О. Інформаційна теорія доказів та проблеми використання електронних засобів доказування у кримінальному процесі. *Journal of the National Academy of Legal Sciences of Ukraine.* 2019. Vol. 26. No. 2. URL: https://visnyk.kh.ua/web/uploads/pdf/%D0%92%D1%96%D1%81%D0%BD%D0%B8%D0%BA_2_2019_%D0%B6%D1%83%D1%80%D0%BD%D0%B0%D0%BB_eng-118-130.pdf

127. Як працює система електронного кримінального провадження «іКейс». *Трансперенсі Інтернешнл Україна*. 2024. URL: https://ti-ukraine.org/research/yak-pratsyuye-systema-elektronnogo-kryminalnogo-provadzhennya-ikejs/

128. Яновська О. Правові позиції Верховного Суду щодо доказів у кримінальних провадженнях : презентація. URL: https://court.gov.ua/storage/portal/supreme/prezentacii_2025/Prezent_Dokazu_krim_provadg.pdf

129. ACPO (Association of Chief Police Officers, UK). Good Practice Guide for Digital Evidence, Version 5.0 October 2011. 43 p.

130. Application/Requête No. 11579/85. Janis KHAN v/the United Kingdom. Janis Khan c/ROYAUME-UNI. URL: https://hudoc.echr.coe.int/eng?i=001-76850

131. Blahuta R. Use of Electronic Evidence in Criminal Proceedings in Ukraine. *Advances in Social Science, Education and Humanities Research.* 2021. Vol. 617.

132. Common Challenges in Cybercrime 2024. The Hague: Europol, 2024. 18 p. *Europol & Eurojust.* URL: https://www.europol.europa.eu/…

133. Commonwealth Draft Model Law on Electronic Evidence. LMM(02)12. URL: https://www.oas.org/juridico/spanish/ cyber/cyb4_evidence_law.pdf

134. Copland v. United Kingdom ECHR 62617/00 (3 April 2007). *Human Rights Law Centre. Case Summaries*. 25.04.2007. URL: https://www.hrlc.org.au/case-summaries/copland-v-united-kingdom-2007-echr-6261700-3-april-2007

135. Cox A. The e-Evidence Package: A New Regime for Cross-Border Law Enforcement Requests. *Arthur Cox – Briefing*. 2024. 2 September. URL: https://www.arthurcox.com/knowledge/the-e-evidence-package-a-new-regime-for-cross-border-law/

136. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. *Official Journal*

of the European Union. 2023. L 191. P. 181–190. URL: https://eur-lex.europa.eu/eli/dir/2023/1544/oj/eng

137. E-evidence Regulation and Directive Published. *Eucrim News.* 2023. URL: https://eucrim.eu/news/e-evidence-regulation-and-directive-published

138. Electronic evidence – a basic guide for First Responders. Good practice material for CERT first responders / Authors of the Study: ENISA, P. Anderson. Council of Europe. Version 3.0. Strasbourg, 2022. 78 c. URL: https://syntheticdrugs.unodc.org/uploads/syntheticdrugs/res/library/cybercrime_html/Electronic_Evidence_A_Basic_Guide_for_First_Responders_ENISA.pdf

139. Esler B.W. Lorraine v. Markel: Unnecessarily raising the standard for admissibility of electronic evidence. *Digital Evidence and Electronic Signature Law Review*. 2007. Vol. 4. P. 80–82. URL: https://sas-space.sas.ac.uk/5473/1/1803-2471-1-SM.pdf

140. Factsheet – Mass surveillance. *European Court of Human Rights*. June 2024. URL: https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng

141. Fair Trials. The Achilles Heel of E-Evidence Regulation (EU) 2023/1543. *Fair Trials – Legal Analysis*. 2025. URL: https://www.fairtrials.org/articles/legal-analysis/the-achilles-heel-of-e-evidence-regulation-eu-2023-1543

142. 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.

143. Grand Chamber judgment in the case of Bărbulescu v. Romania (Application No. 61496/08) : Judgment of the European Court of Human Rights of 5 September 2017. URL: https://www.echr.coe.int/documents/d/echr/press_q_a_barbulescu_eng

144. Jin Du, Liping Ding. Research on the Rules of Electronic Evidence in Chinese Criminal Proceedings. *International Journal of Digital Crime and Forensics*. 2020. Vol. 12. Issue 3. P. 111–121.

145. Juszczak A., Sason E. The Use of Electronic Evidence in the European Area of Freedom, Security and Justice. *EUCRIM*. 2023. Issue 2. P. 182–200. URL:

https://eucrim.eu/articles/the-use-of-electronic-evidence-in-the-european-area-of-freedom-security-and-justice/

146. Kalat D. Nervous System #1: The Thief and the Scientist The Story of the First White Hat Hacker. Legaltech News, February 5. 2018.

147. Khan v. the United Kingdom (Application No. 35394/97) : Judgment of the European Court of Human Rights of 12 May 2000. URL: https://hudoc.echr.coe.int/eng?i=001-58841

148. Lewulis P. Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law. *Criminal Law Forum.* 2022. No. 33. P. 39–62.

149. Metelev O. Problems of determining the admissibility and appropriateness of digital (electronic) evidence in criminal proceedings. *Herald of criminal justice.* 2019. No. 3. P. 224–238. DOI: https://doi.org/10.17721/2413-5372.2019.3/224-238

150. Mifsud Bonnici J. P., Tudorica M., Cannataci J. A. The European Legal Framework on Electronic Evidence: Complex and in Need of Reform. *Law, Governance and Technology Series.* 2018. No. 39. P. 189–234.

151. Murzo Ye. O., Galchenko V. S. Electronic document as an object of forensic examination during the investigation of marauding. *Криміналістика і судова експертиза*. 2024. Вип. 69. С. 258–269. DOI: 10.33994/kndise.2024.69.24

152. Murzo Ye., Halchenko V. Electronic evidence as a means of proof during the pillage investigation. *Scientific Journal of the National Academy of Internal Affairs*. 2023. Vol. 28. No. 3. P. 48–57. DOI: https://doi.org/10.56215/naia-herald/3.2023.48

153. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. *Official Journal of the European Union*. 2023. L 191. P. 118–180. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj

154. Sachoulidou A. Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation. *New Journal of European Criminal Law.* 2024. Vol. 15 (3). P. 256–274. DOI: 10.1177/20322844241258649

155. Šalčius M. The Problem of Obtaining Evidence from EU Countries while Applying Mutual Recognition and Cross-Border Cooperation. *Baltic Journal of Law & Politics.* 2024. Vol. 17 (2). P. 1–21. DOI: 10.2478/bjlp-2024-00022

156. Second Additional Protocol to the Convention on Cybercrime on enhanced Co-operation and Disclosure of Electronic Evidence. Strasbourg, May 12, 2022. URL: https://www.wipo.int/wipolex/en/treaties/details/19810

157. Shumylo M. Ye., Kaplina V. A., Jurka R. Informational Theory of Evidence and the Problems of Using The Electronic Means of Proving in Criminal Procedure. *Journal of the National Academy of Legal Sciences of Ukraine.* 2019. Vol. 26. No. 2. P. 118–130. URL: https://visnyk.kh.ua/web/uploads/pdf/%D0%92%D1%96%D1%81%D0%BD%D0%B8%D0%BA_2_2019_%D0%B6%D1%83%D1%80%D0%BD%D0%B0%D0%BB_eng-118-130.pdf

158. Supreme Court judge speaks about case law on evaluation of electronic evidence in criminal proceedings within the HELP course 'Cybercrime and Electronic Evidence'. URL: https://court.gov.ua/eng/supreme/pres-centr/news/1750192/

159. Topalnakos P. Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings. *Eucrim*. 2023. No. 2. P. 200–204. URL: https://eucrim.eu/articles/critical-issues-in-the-new-eu-regulation-on-electronic-evidence-in-criminal-proceedings/

160. Wahl T. E-evidence Regulation and Directive Published. *Eucrim*. 2023. No. 2. P. 165–168. URL: https://eucrim.eu/news/e-evidence-regulation-and-directive-published/

161. Wynn-Evans C., Byford E. Employee privacy and monitoring. *Dechert LLP.* 2017. URL: https://www.dechert.com/knowledge/onpoint/2017/9/employee-privacy-and-monitoring.html

162. Zakharov v. Russia (European Court of Human Rights, Grand Chamber, Application no. 47143/06, 4 December 2015) : Secret surveillance in Russia violates the right to privacy. *Human Rights Law Centre. Case Summaries*. 2015. URL: https://www.hrlc.org.au/case-summaries/secret-surveillance-in-russia-violates-the-right-to-privacy/

163. Zapf D., Málaga F. EU breaks down digital borders: New e-Evidence rules facilitate cross-border investigations. *White & Case.* 2023. URL: https://www.whitecase.com/insight-alert/eu-breaks-down-digital-borders-new-e-evidence-rules-facilitate-cross-border

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ НАУКОВИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЙНОГО ДОСЛІДЖЕННЯ

Праці, у яких опубліковано основні наукові результати дисертації:

1. Murzo Ye. O., Galchenko V. S. Electronic document as an object of forensic examination during the investigation of marauding. *Криміналістика і судова експертиза*. 2024. Вип. 69. С. 258–269. DOI: 10.33994/kndise.2024.69.24

2. Murzo Ye., Halchenko V. Electronic evidence as a means of proof during the pillage investigation. *Scientific Journal of the National Academy of Internal Affairs*. 2023. Vol. 28. No. 3. P. 48–57. DOI: https://doi.org/10.56215/naia-herald/3.2023.48

3. Гальченко В. С. Міжнародно-правовий досвід використання електронних доказів як засобу доказування у кримінальному провадженні. *Науковий вісник Дніпровського державного університету внутрішніх справ*. 2026. № 1. С. 269–274. DOI: https://doi.org/10.32782/2078-3566-2026-1-35

4. Гальченко В. С. Особливості доказування на підставі електронних доказів: судова практика. *Вісник Кримінологічної асоціації України.* 2026. Т. 38. № 1 (Part II). С. 386–396. DOI: https://doi.org/10.32631/vca.2026.1.p2.35

5. Гальченко В. С. Вилучення та процесуальне оформлення електронних доказів під час проведення досудового розслідування. *Вісник Кримінологічної асоціації України.* 2026. Т. 36. № 2 (Part I). С. 223–233. DOI: https://doi.org/10.32631/vca.2026.2.p1.17

Праці, які засвідчують апробацію матеріалів дисертації:

1. Гальченко В. С. Докази й доказування в кримінальному процесі під час дії воєнного стану. *Кримінальне судочинство: права людини під час дії надзвичайного або воєнного стану* : матеріали Міжнар. наук.-практ. конф.

(Київ, 18 листоп. 2022 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2022. С. 218–220.

2. Гальченко В. С. Проблемні питання допустимості електронних доказів на досудовому слідстві. *Кримінальне судочинство: сучасний стан та перспективи розвитку* : матеріали міжвідом. наук.-практ. конф. (Київ, 28 квіт. 2023 р.) / редкол.: С. С. Чернявський, Я. Ю. Конюшенко, В. В. Корольчук, Ю. В. Сухомлин. Київ : Нац. акад. внутр. справ, 2023. С. 43–46.

3. Гальченко В. С., Мурзо Є. О. Належність і допустимість електронних доказів, отриманих під час розслідування кримінального правопорушення за ст. 432 КК України. *Кримінальне процесуальне право на сучасному етапі розвитку України* : матеріали круглого столу, присвяч. 40-річчю кафедри крим. процесу (Київ, 27 жовт. 2023 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2023. С. 204–207.

4. Гальченко В. С. Електронні докази в кримінальному процесі. *Кримінальне судочинство: сучасний стан та перспективи розвитку* : матеріали Всеукр. наук.-практ. конф., присвяч. пам’яті проф. Ю. І. Азарова (Київ, 2 трав. 2024 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2024. С. 193–195.

Додаток Б

АКТИ ВПРОВАДЖЕННЯ В ПРАКТИЧНУ, НАУКОВУ ДІЯЛЬНІСТЬ, ОСВІТНІЙ ПРОЦЕС

ЗАТВЕРДЖУЮ
Заступник начальника Головного слідчого управління Національної поліції України – начальник управління організації роботи та методичного забезпечення, д. ю. н., професор, заслужений юрист України
полковник поліції

Артем ШЕВЧИШЕН

08. 07 2025 року

АКТ № 65 345 - 2025

Про впровадження у практичну діяльність Головного слідчого управління Національної поліції України *результатів дисертаційного* дослідження Гальченко В.С.

Уклала комісія у складі:

Голови: заступника начальника управління організації роботи та методичного забезпечення Головного слідчого управління Національної поліції України, полковника поліції Ананченка Володимира

членів комісії: начальника 3-го відділу (методичної роботи та правового забезпечення) управління організації роботи та методичного забезпечення Головного слідчого управління Національної поліції України, доктора філософії в галузі права, майора поліції Романова Максима

старшого слідчого в ОВС 3-го відділу (методичної роботи та правового забезпечення) управління організації роботи та методичного забезпечення Головного слідчого управління Національної поліції України, доктора філософії в галузі права, майора поліції Крушеницького Андрія

комісія відповідно до наказу Національної поліції України № 692 від 17.06.2025 «Про затвердження Порядку участі працівників слідчих підрозділів Національної поліції України в науковій та освітній діяльності»,

склала цей акт щодо розгляду основних положень та результатів дисертаційного дослідження Гальченко Вікторії Сергіївни на тему: «Належність та допустимість електронних доказів у кримінальному провадженні», поданого на здобуття ступеня доктора філософії за спеціальністю 081 – Право.

Дисертація присвячена дослідженню теоретичних і практичних аспектів належності та допустимості електронних доказів у кримінальному провадженні. У роботі аналізуються загальні підходи до оцінки електронних доказів, питання їхнього процесуального статусу та вимоги до збирання, фіксації й перевірки. Також розглядаються напрями вдосконалення правового регулювання для забезпечення ефективного використання електронних доказів у кримінальному процесі з дотриманням принципів законності та захисту прав людини.

Комісією встановлено, що висновки, які містяться у дисертаційному дослідженні, можуть використовуватись у практичній діяльності слідчих підрозділів Національної поліції України під час проведення занять у системі службової підготовки, а також при проведенні нарад, семінарів, а викладені у них пропозиції та рекомендації можуть бути корисними під час розслідування кримінальних правопорушень проти власності.

Матеріали, викладені у висновках до дисертаційного дослідження, можуть використовуватись під час підготовки листів-роз'яснень до органів досудового розслідування України, оскільки мають як необхідний теоретичний та методологічний рівень, так і практичну цінність, що сприятиме вдосконаленню їх процесуальної діяльності.

Голова комісії: **Володимир АНАНЧЕНКО**

Члени комісії: **Максим РОМАНОВ**

Андрій КРУШЕНИЦЬКИЙ

ЗАТВЕРДЖУЮ
Проректор Національної академії внутрішніх справ,
доктор юридичних наук, професор
полковник поліції

Олег ТАРАСЕНКО

2026 р.

АКТ

19 . 05 .2026 м. Київ № 167-НД

Впровадження результатів дисертації Гальченко Вікторії Сергіївни «Належність і допустимість електронних доказів у кримінальному провадженні» в наукову діяльність НАВС

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі:

– т.в.о. начальника відділу організації наукової діяльності, кандидата юридичних наук капітана поліції Горбенко Дар'ї Андріївни;

– завідувача науково-дослідної лабораторії з проблем протидії злочинності навчально-наукового інституту поліцейської діяльності, доктора юридичних наук, професора майора поліції Вознюка Андрія Андрійовича;

– начальника відділу аспірантури (ад'юнктури) і докторантури, доктора юридичних наук, професора підполковника поліції Тихонової Олени Вікторівни;

– завідувача кафедри кримінального процесу, доктора юридичних наук, професора підполковника поліції Таран Олени Вікторівни;

– завідувача загальної бібліотеки Гайдар Людмили Георгіївни.

Комісія розглянула й узагальнила наукові праці ад'юнкта денної форми навчання кафедри кримінального процесу Національної академії внутрішніх Гальченко Вікторії Сергіївни «Належність і допустимість електронних доказів у кримінальному провадженні» поданої на здобуття наукового ступеня доктора юридичних наук зі спеціальності 081 – Право та на основі проведеного аналізу зробила висновок, що надана наукові праці містить низку обґрунтованих теоретичних положень і пропозицій спрямованих на теоретичне дослідження належності і допустимості електронних доказів у кримінальному провадженні.

Проаналізовано основні результати дослідження Гальченко В.С., зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

1. Murzo, Ye., & Halchenko, V. (2023). Electronic evidence as a means of proof during the pillage investigation. Scientific Journal of the National Academy of Internal Affairs, 28(3), 48-57. https://doi.org/10.56215/naia-herald/3.2023.48.

2. Murzo, Ye. O., Galchenko V. S. (2024). Electronic document as an object of forensic examination during the investigation of marauding. *Криміналістика і судова експертиза*. Вип. 69. С. 258-269. DOI: 10.33994/kndise.2024.69.24

3. Гальченко В.С. Міжнародно-правовий досвід використання електронних доказів як засобу доказування у кримінальному провадженні. *Науковий вісник Дніпровського державного університету внутрішніх справ: науковий журнал*. 2026. № 1. с. 269–274. https://doi.org/10.32782/2078-3566-2026-1-35

4. Гальченко В.С. Особливості доказування на підставі електронних доказів: судова практика. (2026). *Вісник Кримінологічної асоціації України*, *38*(1 (Part II), 386-396. https://doi.org/10.32631/vca.2026.1.p2.35

5. Гальченко В.С. Вилучення та процесуальне оформлення електронних доказів під час проведення досудового розслідування. (2026). *Вісник Кримінологічної асоціації України*, *39*(2 (Part I), 223-233. https://doi.org/10.32631/vca.2026.2.p1.17

6. Гальченко В.С. Докази й доказування в кримінальному процесі під час дії воєнного стану Кримінальне судочинство: права людини під час дії надзвичайного або воєнного стану [Текст] : матеріали Міжнар. наук.-практ. конф. (Київ, 18 листоп. 2022 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. – Київ : Нац. акад. внутр. справ, 2022. С. 218-220.

7. Гальченко В.С. Проблемні питання допустимості електронних доказів на досудовому слідстві. Кримінальне судочинство: сучасний стан та перспективи розвитку [Текст] : матеріали міжвідом. наук.-практ. конф. (Київ, 28 квіт. 2023 р.) / [редкол.: С. С. Чернявський, Я. Ю. Конюшенко, В. В. Корольчук Ю. В. Сухомлин]. – Київ : Нац. акад. внутр. справ, 2023. С. 43-46.

8. Гальченко В.С., Мурзо Є.О. Належність і допустимість електронних доказів, отриманих під час розслідування кримінального правопорушення за ст. 432 КК України. Кримінальне процесуальне право на сучасному етапі розвитку України [Текст] : матеріали круглого столу, присвяч. 40-річчю кафедри кримінального процесу (Київ, 27 жовт. 2023 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. – Київ : Нац. акад. внутр. справ, 2023. С. 204-207.

9. Гальченко В.С. Електронні докази в кримінальному процесі. Кримінальне судочинство: сучасний стан та перспективи розвитку [Текст] : матеріали Всеукраїнської науково- практичної конференції, присвяч. пам'яті професора Ю.І. Азарова (Київ, 2 трав. 2024 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. – Київ : Нац. акад. внутр. справ, 2024. С. 193-195.

На основі проведеного аналізу комісія зробила висновок про те, що вищезазначені матеріали Гальченко В.С. можуть застосовуватися під час підготовки монографій, підручників, навчальних посібників, методичних рекомендацій, узагальнення аналітичних матеріалів, обґрунтування пропозицій до чинних проєктів нормативно-правових актів, підготовка яких потребує проведення відповідних наукових досліджень або містить наукову складову.

Члени комісії: **Дар'я ГОРБЕНКО**

Андрій ВОЗНЮК

Олена ТИХОНОВА

Олена ТАРАН

Людмила ГАЙДАР

ЗАТВЕРДЖУЮ
Проректор Національної
академії внутрішніх справ
доктор юридичних наук, професор
полковник поліції

Сергій ЧЕРНЯВСЬКИЙ

2026 р.

АКТ

19.05.2026 м. Київ № 166-ОП

Впровадження результатів дисертації Гальченко Вікторії Сергіївни «Належність і допустимість електронних доказів у кримінальному провадженні» в освітній процес НАВС

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі:

– заступника начальника відділу організації освітнього процесу, кандидата юридичних наук, старшого наукового співробітника полковника поліції Корольчука Віктора Володимировича;

– т.в.о. начальника відділу організації наукової діяльності, кандидата юридичних наук капітана поліції Горбенко Дар'ї Андріївни;

– начальника відділу аспірантури (ад'юнктури) і докторантури, доктора юридичних наук, професора підполковника поліції Тихонової Олени Вікторівни;

– завідувача кафедри кримінального процесу, доктора юридичних наук, професора підполковника поліції Таран Олени Вікторівни;

– завідувача загальної бібліотеки Гайдар Людмили Георгіївни.

Комісія розглянула й узагальнила наукові праці ад'юнкта денної форми навчання кафедри кримінального процесу Національної академії внутрішніх Гальченко Вікторії Сергіївни «Належність і допустимість електронних доказів у кримінальному провадженні» поданої на здобуття наукового ступеня доктора юридичних наук зі спеціальності 081 – Право.

Проаналізовано основні результати дослідження Гальченко В.С. зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

1. Murzo, Ye., & Halchenko, V. (2023). Electronic evidence as a means of proof during the pillage investigation. Scientific Journal of the National Academy of Internal Affairs, 28(3), 48-57. https://doi.org/10.56215/naia-herald/3.2023.48.
2. Murzo, Ye. O., Galchenko V. S. (2024). Electronic document as an object of forensic examination during the investigation of marauding. *Криміналістика і судова експертиза*. Вип. 69. С. 258-269. DOI: 10.33994/kndise.2024.69.24
3. Гальченко В.С. Міжнародно-правовий досвід використання електронних доказів як засобу доказування у кримінальному провадженні. *Науковий вісник Дніпровського державного університету внутрішніх справ: науковий журнал*. 2026. № 1. с. 269–274. https://doi.org/10.32782/2078-3566-2026-1-35

4. Гальченко В.С. Особливості доказування на підставі електронних доказів: судова практика. (2026). *Вісник Кримінологічної асоціації України*, *38*(1 (Part II), 386-396. https://doi.org/10.32631/vca.2026.1.p2.35

5. Гальченко В.С. Вилучення та процесуальне оформлення електронних доказів під час проведення досудового розслідування. (2026). *Вісник Кримінологічної асоціації України*, *39*(2 (Part I), 223-233. https://doi.org/10.32631/vca.2026.2.p1.17

6. Гальченко В.С. Докази й доказування в кримінальному процесі під час дії воєнного стану Кримінальне судочинство: права людини під час дії надзвичайного або воєнного стану [Текст] : матеріали Міжнар. наук.-практ. конф. (Київ, 18 листоп. 2022 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. – Київ : Нац. акад. внутр. справ, 2022. С. 218-220.

7. Гальченко В.С. Проблемні питання допустимості електронних доказів на досудовому слідстві. Кримінальне судочинство: сучасний стан та перспективи розвитку [Текст] : матеріали міжвідом. наук.-практ. конф. (Київ, 28 квіт. 2023 р.) / [редкол.: С. С. Чернявський, Я. Ю. Конюшенко, В. В. Корольчук Ю. В. Сухомлин]. – Київ : Нац. акад. внутр. справ, 2023. С. 43-46.

8. Гальченко В.С., Мурзо Є.О. Належність і допустимість електронних доказів, отриманих під час розслідування кримінального правопорушення за ст. 432 КК України. Кримінальне процесуальне право на сучасному етапі розвитку України [Текст] : матеріали круглого столу, присвяч. 40-річчю кафедри кримінального процесу (Київ, 27 жовт. 2023 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. – Київ : Нац. акад. внутр. справ, 2023. С. 204-207.

9. Гальченко В.С. Електронні докази в кримінальному процесі. Кримінальне судочинство: сучасний стан та перспективи розвитку [Текст] : матеріали Всеукраїнської науково- практичної конференції, присвяч. пам'яті професора Ю.І. Азарова (Київ, 2 трав. 2024 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. – Київ : Нац. акад. внутр. справ, 2024. С. 193-195.

На основі проведеного аналізу комісія зробила висновок, що праці Гальченко В.С. містять науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання в освітньому процесі Національної академії внутрішніх справ, зокрема при викладанні навчальних дисциплін «Кримінальний процес», «Процесуальні документи в кримінальному провадженні», «Складання процесуальних документів на стадії досудового розслідування», під час підготовки навчально-методичних та дидактичних матеріалів, а також рекомендувати їх до вивчення під час самостійної роботи здобувачів вищої освіти.

Члени комісії: **Віктор КОРОЛЬЧУК**

Дар'я ГОРБЕНКО

Олена ТИХОНОВА

Олена ТАРАН

Людмила ГАЙДАР

Додаток В

АНКЕТА

Шановний(а) респонденте!

Просимо Вас взяти участь в анонімному опитуванні, метою якого є вивчення практики використання електронних доказів у кримінальному провадженні та проблемних питань, що виникають під час роботи з ними. Отримані результати будуть використані виключно в наукових цілях.

1. Ваш процесуальний статус:

а) слідчий;

б) прокурор;

в) адвокат.

2. Стаж Вашої професійної діяльності?

а) до 3 років;

б) від 3 до 5 років;

в) від 5 до 10років;

г) понад 10 років.

3. Чи підтримуєте Ви запровадження окремої статті КПК України, яка б містила визначення поняття «електронні (цифрові) докази»?

а) так;

б) ні.

4. Чи є доцільним законодавче закріплення таких видів електронних доказів, як абонентські дані, трафік-дані та контент-дані?

а) доцільно;

б) недоцільно.

5. Чи виникали у Вашій практиці труднощі з визначенням процесуального статусу електронних даних як доказів?

а) так;

б) ні.

6. Чи підтримуєте Ви запровадження обов'язкового протоколу вилучення, копіювання та отримання електронних (цифрових) даних із зазначенням способу отримання, технічних засобів та хеш-значень файлів?

а) так;

б) ні.

7. Чи виникали у Вас випадки визнання електронних доказів недопустимими?

а) так, неоднарозово;

б) так, поодинокі випадки;

в) ні;

г) важко відповісти.

8. Які причини найчастіше призводять до сумнівів щодо допустимості електронних доказів? *(оберіть варіант, який трапляється найчастіше)*

а) Порушення порядку отримання;

б) Неналежна фіксація в протоколах;

в) Неможливість підтвердити автентичність даних.

9. Чи підтримуєте Ви розширення використання цифрових технологій та електронних доказів у кримінальному провадженні?

а) так;

б) ні.

10. Які критерії, на Вашу думку, повинні бути основними для оцінки допустимості електронних (цифрових) доказів?

а) законність отримання;

б) автентичність даних;

в) цілісність даних;

г) належне документування процесу отримання;

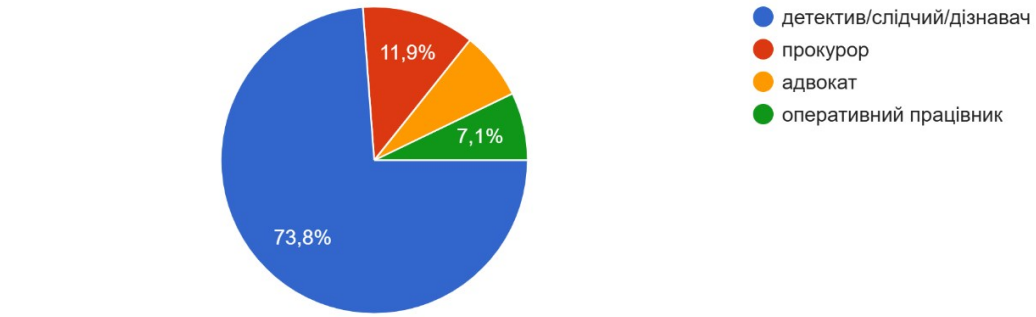
д) відповідність вимогам захисту прав людини.

ЗВЕДЕНІ ДАНІ

результатів анкетування прокурорів, суддів, слідчих, дізнавачів, адвокатів та інших фахівців у галузі права (42 особи)

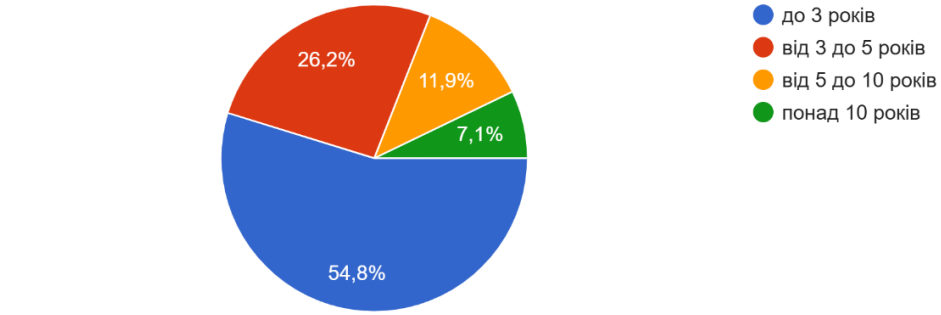
Ваш процесуальний статус

42 ответа



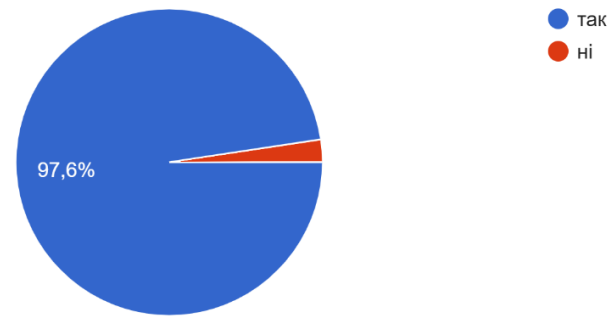
Стаж Вашої професійної діяльності?

42 ответа



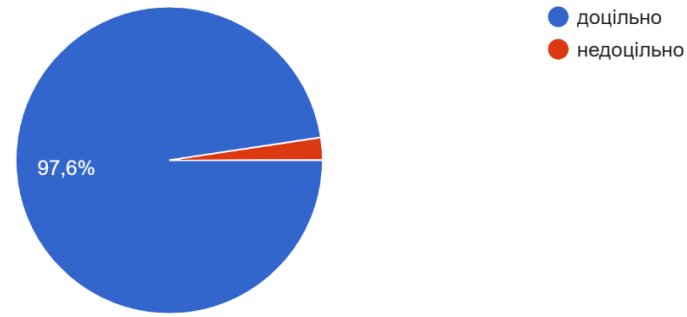
Чи підтримуєте Ви запровадження окремої статті КПК України, яка б містила визначення поняття «електронні (цифрові) докази»?

42 ответа



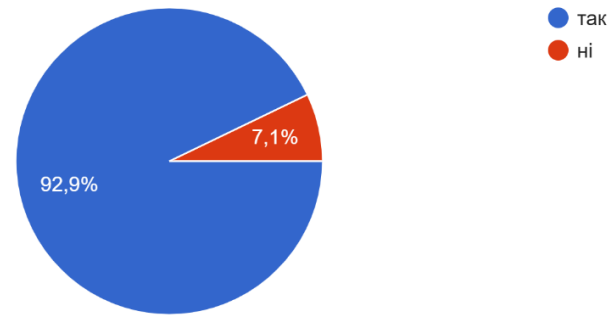
Чи є доцільним законодавче закріплення таких видів електронних доказів, як абонентські дані, трафік-дані та контент-дані?

42 ответа

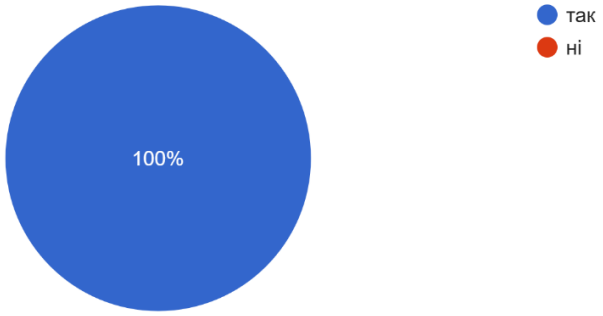


Чи виникали у Вашій практиці труднощі з визначенням процесуального статусу електронних даних як доказів?

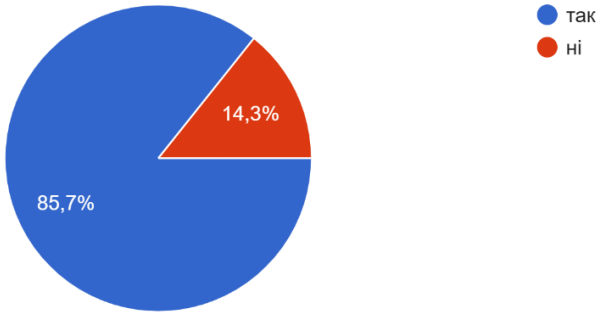
42 ответа



Чи підтримуєте Ви запровадження обов'язкового протоколу вилучення, копіювання та отримання електронних (цифрових) даних із заз...ння, технічних засобів та хеш-значень файлів?
42 ответа



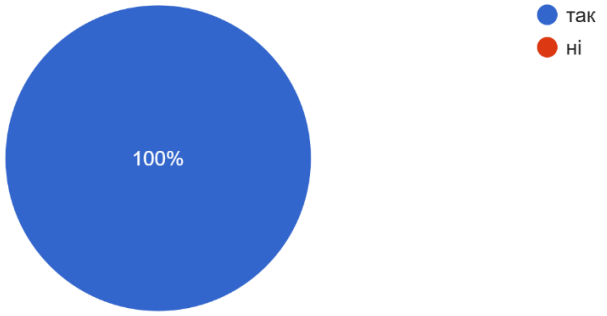
Чи виникали у Вас випадки визнання електронних доказів недопустимими?
42 ответа



Які причини найчастіше призводять до сумнівів щодо допустимості електронних доказів? (оберіть варіант, який трапляється найчастіше)
42 ответа

Чи підтримуєте Ви розширення використання цифрових технологій та електронних доказів у кримінальному провадженні?

42 ответа



Які критерії, на Вашу думку, повинні бути основними для оцінки допустимості електронних (цифрових) доказів?

42 ответа

Додаток Г

ПРОПОЗИЦІЇ ЩОДО ВНЕСЕННЯ ЗМІН ДО КРИМІНАЛЬНОГО ПРОЦЕСУАЛЬНОГО КОДЕКСУ УКРАЇНИ

Зміст положення (норми) чинного акта законодавства	**Зміст відповідного положення (норми) в запропонованій редакції**
Кримінальний процесуальний кодекс України	
Норма відсутня.	**Стаття 99-1. Електронні (цифрові) докази** **1. Електронними (цифровими) доказами є інформація в електронній (цифровій) формі, що містить відомості про обставини, які підлягають доказуванню у кримінальному провадженні.** **2. До електронних (цифрових) доказів належать, зокрема, такі види електронних даних:** **1) абонентські дані;** **2) трафік-дані;** **3) контент-дані.** **3. Електронні (цифрові) докази можуть зберігатися на електронних носіях, у комп'ютерних системах, інформаційно-телекомунікаційних мережах або інших цифрових середовищах.**
Норма відсутня.	**Стаття 104-1. Протокол вилучення, копіювання та отримання електронних (цифрових) даних** **1. Під час вилучення, копіювання або отримання електронних (цифрових) даних складається протокол.** **2. У протоколі зазначаються:**

	спосіб отримання електронних даних; **технічні засоби, що використовувалися під час вилучення або копіювання;** **опис джерела отримання даних;** **цифрові ідентифікатори та контрольні хеш-значення електронних даних;** **інші відомості, необхідні для підтвердження цілісності та автентичності даних.** **3. Недодержання вимог цієї статті може бути підставою для визнання відповідного доказу недопустимим.**
Стаття 85. Належність доказів 1. Належними є докази, які прямо чи непрямо підтверджують існування чи відсутність обставин, що підлягають доказуванню у кримінальному провадженні, та інших обставин, які мають значення для кримінального провадження, а також достовірність чи недостовірність, можливість чи неможливість використання інших доказів. **Положення відсутні.**	**Стаття 85.** Належність доказів 1. Належними є докази, які прямо чи непрямо підтверджують існування чи відсутність обставин, що підлягають доказуванню у кримінальному провадженні, та інших обставин, які мають значення для кримінального провадження, а також достовірність чи недостовірність, можливість чи неможливість використання інших доказів. **Електронні (цифрові) докази визнаються належними, якщо з урахуванням їх виду (абонентські дані, трафік-дані, контент-дані) вони прямо або опосередковано підтверджують чи спростовують обставини, що підлягають доказуванню у кримінальному провадженні.**
Стаття 87. Недопустимість доказів, отриманих внаслідок істотного порушення прав та свобод людини …	**Стаття 87.** Недопустимість доказів, отриманих внаслідок істотного порушення прав та свобод людини …

4. Докази, передбачені цією статтею, повинні визнаватися судом недопустимими під час будь-якого судового розгляду, крім розгляду, якщо вирішується питання про відповідальність за вчинення зазначеного істотного порушення прав та свобод людини, внаслідок якого такі відомості були отримані. **Положення відсутні.** **…**	4. Докази, передбачені цією статтею, повинні визнаватися судом недопустимими під час будь-якого судового розгляду, крім розгляду, якщо вирішується питання про відповідальність за вчинення зазначеного істотного порушення прав та свобод людини, внаслідок якого такі відомості були отримані. **Електронні (цифрові) докази визнаються допустимими, якщо вони отримані у спосіб, що забезпечує їх цілісність, автентичність та можливість перевірки, а також у обсязі, необхідному і достатньому для досягнення мети кримінального провадження** **…**